

网络卫士安全网关管理手册 ——基础配置



天融信
TOPSEC®

北京市海淀区上地东路 1 号华控大厦 100085

电话: +8610-82776666

传真: +8610-82776677

服务热线: +8610-8008105119

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

版权声明

本手册中的所有内容及格式的版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有 不得翻印 © 2011 天融信公司

商标声明

本手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC® 天融信公司

信息反馈

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

目 录

1	前言	1
1.1	文档目的	1
1.2	读者对象	1
1.3	约定	1
1.4	相关文档	2
1.5	扩展功能	2
1.6	技术服务体系	3
2	网络卫士安全网关简介	4
2.1	功能和特点	4
2.2	工作原理	5
2.2.1	处理数据流	5
2.2.2	匹配访问控制规则	9
2.3	工作模式	10
2.3.1	路由模式	10
2.3.2	透明模式	11
2.3.3	混合模式	12
2.4	虚系统	12
3	安全网关初始配置和管理方式	14
3.1	出厂配置	14
3.1.1	缺省管理用户	14
3.1.2	缺省空闲超时	14
3.1.3	缺省系统参数	14
3.1.4	缺省日志服务器	15
3.1.5	缺省接口配置	15
3.1.6	缺省地址对象	15
3.1.7	缺省区域对象	15
3.1.8	本机服务访问控制规则	15
3.2	工作状态	16
3.3	管理方式	16
3.3.1	通过CONSOLE口管理网络卫士安全网关	16
3.3.2	设置其他管理方式	18
3.3.2.1	设置接口IP地址	18
3.3.2.2	定义地址对象	19
3.3.2.3	指定管理方式	19
3.3.2.4	设置管理方式实例	20
3.3.3	管理主机的相关设置	21
3.4	通过浏览器登录安全网关	22
3.5	初始配置向导	22
3.5.1	ADSL配置向导	23
3.5.2	固定IP配置向导	28
4	系统管理	35
4.1	基本信息	35
4.2	配置	41
4.2.1	设置系统参数	42
4.2.2	开放服务	44
4.2.2.1	管理系统服务	45
4.2.2.2	开放服务	45
4.2.3	设置系统时间	47

4.2.4	SNMP.....	49
4.2.4.1	SNMP代理服务控制.....	49
4.2.4.2	管理主机.....	50
4.2.4.3	陷阱主机.....	51
4.2.4.4	SNMPV3 用户.....	52
4.2.5	邮件设置.....	53
4.2.6	短信设置.....	54
4.2.7	WEB 管理.....	55
4.2.8	TP 注册.....	56
4.3	维护.....	58
4.3.1	配置维护.....	58
4.3.2	系统升级.....	62
4.3.3	重启.....	64
4.3.4	健康记录.....	65
4.3.5	诊断.....	65
4.3.6	服务更新.....	66
4.3.6.1	更新病毒库及许可证.....	67
4.3.6.2	更新入侵防御规则库.....	69
4.3.6.3	更新应用识别规则库.....	70
4.3.6.4	更新URL库.....	71
4.4	配置系统管理员.....	72
4.4.1	配置管理员账号.....	73
4.4.2	配置管理权限.....	75
4.4.3	设置.....	77
5	系统监视.....	79
5.1	连接信息.....	79
5.2	接口流量.....	80
5.3	攻击统计.....	82
5.4	攻击排名.....	83
5.4.1	攻击排名.....	83
5.4.2	受攻击主机排名.....	84
5.5	应用统计.....	85
5.5.1	传统协议.....	87
5.5.2	股票交易.....	87
5.5.3	即时通讯.....	88
5.5.4	流媒体.....	88
5.5.5	网络游戏.....	89
5.5.6	网络电话.....	89
5.5.7	网络电视.....	90
5.5.8	P2P 下载.....	90
5.5.9	其他流量.....	91
5.5.10	自定义协议.....	91
5.6	应用排名.....	92
5.6.1	应用排名.....	92
5.6.2	应用主机排名.....	93
5.7	病毒统计.....	95
5.8	病毒排名.....	97
5.8.1	病毒排名.....	97
5.8.2	感染病毒主机排名.....	98
5.8.3	病毒来源排名.....	99
6	网络管理.....	100
6.1	网络规划.....	100

6.2	接口设置.....	102
6.2.1	物理接口.....	103
6.2.2	子接口.....	106
6.3	二层网络.....	109
6.3.1	ARP.....	109
6.3.2	VLAN.....	110
6.3.2.1	添加VLAN到安全网关设备.....	111
6.3.2.2	设定VLAN虚接口的属性.....	112
6.3.2.3	生成树属性设置.....	113
6.3.3	MAC.....	115
6.4	路由.....	116
6.4.1	路由表.....	117
6.4.2	策略路由.....	119
6.4.3	动态路由OSPF.....	123
6.4.3.1	启动或停止OSPF服务.....	123
6.4.3.2	查看OSPF协议配置信息.....	125
6.4.3.3	配置路由ID.....	125
6.4.3.4	设置区域.....	126
6.4.3.5	重新发布路由.....	126
6.4.3.6	设置ACL.....	128
6.4.3.7	设置ACL分发规则.....	129
6.4.3.8	设置接口属性.....	130
6.4.4	动态路由RIP.....	131
6.4.4.1	启动或停止RIP协议.....	131
6.4.4.2	查看RIP协议配置信息.....	132
6.4.4.3	设置网络.....	133
6.4.4.4	设置邻居.....	133
6.4.4.5	重新发布.....	134
6.4.5	动态路由BGP.....	135
6.4.5.1	启动或停止BGP协议.....	135
6.4.5.2	查看BGP协议配置信息.....	136
6.4.5.3	配置路由ID.....	137
6.4.5.4	宣告网段.....	137
6.4.5.5	邻居.....	138
6.4.5.6	重新发布信息.....	139
6.4.5.7	地址聚合.....	140
6.4.6	多播路由.....	141
6.5	接入.....	142
6.5.1	ADSL.....	142
6.5.2	虚拟线.....	145
6.5.3	链路聚合.....	146
6.5.4	802.1X认证.....	149
6.5.5	VLAN-VPN.....	150
6.6	DHCP.....	152
6.6.1	安全网关作为DHCP服务器.....	152
6.6.2	安全网关作为DHCP客户端.....	156
6.6.3	安全网关作为DHCP中继.....	158
6.7	流量管理.....	159
6.7.1	QoS.....	159
6.7.2	地址统计.....	163
6.7.3	常用端口流量统计.....	166
6.7.4	IP连接统计.....	168
6.8	IP探测.....	169
6.9	域名解析.....	171
7	资源管理.....	172

7.1	设置地址资源.....	172
7.1.1	设置主机资源.....	172
7.1.2	设置地址范围资源.....	175
7.1.3	设置子网资源.....	176
7.1.4	设置地址组.....	177
7.2	设置区域资源.....	179
7.3	设置时间资源.....	180
7.3.1	设置多次时间对象.....	180
7.3.2	设置单次时间对象.....	181
7.4	设置服务资源.....	183
7.4.1	预定义服务.....	183
7.4.2	自定义服务.....	183
7.4.3	设置服务组.....	184
7.5	设置域名对象.....	185
8	用户认证.....	188
8.1	用户管理.....	189
8.1.1.1	配置用户.....	190
8.1.1.2	查看在线用户.....	194
8.1.1.3	用户设置.....	195
8.2	用户角色设置.....	196
8.2.1	角色管理.....	197
8.2.2	分级管理.....	200
8.3	外部认证.....	201
8.4	认证设置.....	206
8.5	可信接入.....	211
8.5.1	安全规则.....	211
8.5.2	安全规则组.....	214
8.5.3	用户策略.....	216
8.5.4	角色策略.....	217
8.5.5	检查方式.....	218
9	防火墙.....	219
9.1	阻断策略.....	219
9.2	访问控制规则.....	223
9.2.1	查看规则.....	223
9.2.2	查询规则.....	225
9.2.3	管理规则.....	227
9.2.4	添加规则组.....	230
9.2.5	添加规则.....	231
9.3	访问记录.....	235
9.4	地址转换.....	238
9.4.1	基本概念.....	238
9.4.2	查看NAT规则.....	239
9.4.3	添加NAT规则.....	241
9.4.4	改变NAT规则的位置.....	244
9.5	IP/MAC地址绑定.....	244
9.6	内容安全策略.....	248
10	内容过滤.....	261
10.1	邮件过滤.....	261
10.1.1	内容过滤.....	261
10.1.2	警告邮件内容.....	263
10.2	HTTP过滤.....	264

10.2.1	URL过滤.....	264
10.2.2	内容过滤.....	265
10.3	其他协议过滤.....	267
10.3.1	关键字对象.....	267
10.3.2	登录标题对象.....	269
10.4	应用端口绑定.....	270
11	应用识别.....	273
11.1	账号过滤.....	273
11.2	自定义应用.....	275
11.3	主机监控.....	276
11.4	P2P行为识别.....	277
11.5	流量异常检测.....	277
12	PKI设置.....	279
12.1	本机证书.....	279
12.1.1	配置IPSec VPN网关证书.....	280
12.1.2	配置SSL VPN网关证书.....	282
12.2	第三方CA证书.....	283
12.2.1	配置CA根证书.....	284
12.2.2	配置CRL自动下载.....	285
12.3	本地CA策略.....	286
12.3.1	配置内置CA根证书.....	287
12.3.2	签发证书.....	290
12.3.3	证书撤销列表设置.....	297
12.4	USB KEY.....	298
12.5	远程证书认证.....	299
12.6	证书请求.....	300
12.6.1	配置IPSec VPN证书请求.....	300
12.6.2	配置SSL VPN证书请求.....	302
12.7	备份和恢复.....	304
13	虚拟专网.....	306
13.1	L2TP管理.....	306
13.2	PPTP管理.....	308
13.3	GRE管理.....	310
14	入侵防御.....	314
14.1	主机防护.....	314
14.1.1	主机防护.....	314
14.1.2	范围防护.....	316
14.1.3	子网防护.....	317
14.2	主机限制.....	318
14.2.1	主机限制.....	318
14.2.2	范围限制.....	319
14.2.3	子网限制.....	320
14.3	ANTI-DOS.....	321
14.3.1	设置IDS规则.....	322
14.3.2	黑白名单设置.....	324
14.3.3	攻击统计显示.....	326
14.4	防ARP欺骗.....	326
14.5	防路由欺骗.....	327
14.6	IDS联动.....	328

15	反垃圾邮件	332
15.1	黑白名单	332
15.1.1	设置邮件地址黑白名单	332
15.1.2	设置IP地址黑白名单	334
15.2	实时黑名单	336
15.3	灰名单技术	337
15.4	反垃圾统计	338
16	高可用性	340
16.1	接口联动	340
16.2	高可用性	342
16.2.1	双机热备模式	343
16.2.2	负载均衡模式	346
16.2.3	连接保护模式	350
16.3	链路备份	352
16.4	服务器负载均衡	353
16.4.1	定义服务器	354
16.4.2	定义负载均衡组	355
17	日志与报警	358
17.1	日志设置	358
17.2	日志查看	360
17.2.1	常规日志	360
17.2.2	深度内容过滤日志	361
17.2.3	病毒过滤日志	361
17.2.4	反垃圾邮件日志	362
17.2.5	应用程序识别日志	363
17.2.6	IPS日志	363
17.3	报警	364
17.3.1	添加报警规则	364
17.3.2	设置触发报警的安全事件	368
17.3.3	删除报警规则	369
附录 A	常用服务及端口	370
附录 B	简单网络管理协议SNMP	375
附录 C	术语索引	382

1 前言

本用户手册主要介绍网络卫士安全网关的安装、配置、使用和管理。通过阅读本文档，用户可以了解网络卫士安全网关的基本设计思想，并根据实际应用环境安装和配置安全网关。

本章内容主要包括：

- 文档目的
- 读者对象
- 约定
- 相关文档
- 扩展功能
- 技术服务体系

1.1 文档目的

本文档主要介绍如何安装、配置网络卫士安全网关。通过阅读本文档，用户能够正确地安装和配置网络卫士安全网关，并综合运用安全设备提供的多种安全技术，包括访问控制、VPN、入侵检测和 QoS 管理等有效地保护用户网络，控制网络的非法访问和抵御网络攻击，实现高效可靠的安全通信。

1.2 读者对象

本用户手册适用于具有基本网络知识的系统管理员和网络管理员阅读，通过阅读本文档，他们可以独立完成以下一些工作：

- 网络卫士安全网关的基本管理
- 制定各个防火区之间的包过滤策略
- 制定地址转换策略
- 制定访问控制策略
- 设置网络卫士安全网关的各种附加安全引擎，如防病毒安全引擎等。
- 管理与配置网络卫士安全网关的附加功能模块，如备份系统、系统高可用性配置、IDS、QoS 等。

1.3 约定

本文档遵循以下约定：

一级标题前的“*”表示该功能模块不是产品的标准配置模块，而是可选模块。更详细的信息请咨询天融信公司相关人员。

1) 命令语法描述采用以下约定：

尖括号 (<>) 表示该命令参数为必选项。

方括号 ([]) 表示该命令参数是可选项。

竖线 (|) 隔开多个相互独立的备选参数。

黑体表示需要用户输入的命令或关键字，例如**help**命令。

*斜体*表示需要用户提供实际值的参数。

2) 图形界面操作的描述采用以下约定：

“ ” 表示按钮。

点击（选择）一个菜单项采用如下约定：

点击（选择） **高级管理 > 特殊对象 > 用户**。

为了叙述方便，本文档采用了大量网络拓扑图，图中的图标用于指明天融信安全设备和通用的网络设备、外设和其他设备，以下图标注释说明了这些图标代表的设备：



文档中出现的提示、警告、说明、示例等，是关于用户在安装和配置网络卫士安全网关过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。

文档中出现的接口标识 eth1、eth2 等，是为了表示方便，不一定与设备接口名称相对应。

1.4 相关文档

《TopGate 管理手册——IPSEC VPN 配置》

《TopGate 管理手册——SSL VPN 配置》

《TopGate 管理手册——防病毒配置》

《TopGate 管理手册——IPS 配置》

1.5 扩展功能

天融信 TOS 系列产品均具备扩展功能，用户可根据需要对所购买产品进行扩展。各产品扩展功能的详细信息请参见下表：

产品名称	可扩展功能	备注

产品名称	可扩展功能	备注
网络卫士防火墙（NGFW）	IV、SV、AV、IPS、BGP	对于扩展功能的详细说明和获得方式，请向天融信相关人员咨询。
网络卫士 VPN（IPSEC VPN）	AV、IPS、SV	
网络卫士入侵防御系统（IPS）	入侵防御：IDS、IDS_CC、IDBP 内容过滤：HTTP、FTP、POP3、H323、SMTP、RPC、RTSP、MMS、SQLNET、SIP、IMAP、TELNET、DNS、RSH、DPI_AR 其他：IV、SV、AV	
网络卫士安全网关（UTM）	SV	
网络卫士多合一网关（VONE）	AV、IPS	

1.6 技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

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

在线技术资料

<http://www.topsec.com.cn/support/down.asp>

安全解决方案

<http://www.topsec.com.cn/solutions/qw.asp>

技术支持中心

<http://www.topsec.com.cn/support/support.asp>

天融信全国安全服务热线

800-810-5119

2 网络卫士安全网关简介

网络卫士安全网关，是以天融信公司具有自主知识产权的 TOS 操作系统（Topsec Operating System）为系统平台，采用开放性的系统架构及模块化的设计，融合了防火墙、入侵检测、身份认证等多种安全解决方案，构建而成的一个安全、高效、易于管理和扩展的网络卫士安全网关。

TOS 操作系统是天融信自主研发的新一代系统平台，采用全模块化设计、中间层理念，具有高效性、高安全性、高健壮性、扩展性、可移植性、模块化、标准化等特征。同时，TOS 操作系统能够支持多种硬件平台，在 X86、NP、以及 ASIC 等平台上均可以高效、稳定的运行。

本章主要包括：

- 功能和特点：介绍网络卫士安全网关的主要功能和特点。
- 工作原理：介绍网络卫士安全网关的工作原理，主要包括处理数据流和匹配访问控制规则。
- 工作模式：介绍网络卫士安全网关的路由、透明以及混合工作模式。

2.1 功能和特点

网络卫士安全网关本身可以提供完整的访问控制功能，可以自由地采用路由、透明及混合等多种方式集成到客户网络环境中，并通过与天融信的其他安全产品相配合，为客户网络提供强大的安全保护功能。同时，客户还可以通过原有的网络管理平台（如 SNMP 管理器或日志服务器）对网络卫士安全网关的运行状况进行查询、监控和日志分析。另外，网络卫士安全网关还提供了与其他厂家安全产品的联动功能（如入侵检测系统），极大地方便了系统功能的扩展。

网络卫士安全网关具有如下基本功能：

- 支持透明、路由和混合三种工作模式。
- 支持基于对象的网络访问控制，包括网络层、应用层等多层次的访问控制；支持 URL、HTTP 脚本、关键字、邮件等多种形式的内容过滤。
- 支持多种网络地址转换（NAT）方式。
- 支持多种认证方式，如本地认证、证书认证、Radius 认证、TACACS、SecurID、LDAP、域认证等。
- 支持标准 IPSec VPN。
- 内置 IDS 模块，能够自防御 Land、Smurf、TearOfDrop、Ping of Death、SynFlood、Targa3 和 IpSweep 等十几种攻击，具有抗 DOS/DDOS 攻击功能。

- 基于 TOPSEC 协议，实现与 IDS 等多种安全产品的联动。
- 支持网络卫士安全网关双机热备。
- 支持 IPX、NETBEUI、VOD、H.323v1/v2、SSH 协议。
- 支持 DHCP，包括 DHCP SERVER、DHCP CLIENT 以及 DHCP RELAY（中继）。
- 支持 VLAN 与生成树。
- 支持 ADSL 接入与链路备份。
- 支持服务器负载均衡功能。

网络卫士安全网关具有如下特点：

- 采用多接口设计，具有良好的网络应用可扩展性。
- 高效的应用层访问控制。传统的应用层控制采用代理技术，系统需频繁地在系统核心和应用层以及进程之间切换，消耗了大量系统资源，影响性能。网络卫士安全网关采用核检测技术，应用深度过滤策略在系统内核实现应用层深度过滤，并可以实现基于会话的认证。
- 灵活的管理。实现了 TOPSEC 安全网关管理协议，管理员可以从网络卫士安全网关的任何接口登录网络卫士安全网关，实现类似交换机设备的中央管理。
- 全新的管理端口协议。该协议实现了在安全网关的唯一服务端口上同时运行多个管理事务服务。
- 支持基于 TOPSEC 协议的 IDS 和反病毒联动。实现 TOPSEC 联动协议，可与基于 TOPSEC 协议的 IDS 和反病毒产品进行联动，提供智能的网络安全保护。
- 高性能的内容过滤。系统核心层实现传输内容的还原、安全检测，实现高性能的 TOPSEC 内容安全协议，支持病毒检测和垃圾邮件过滤。
- 系统升级与容错。网络卫士安全网关可以通过命令行方式进行系统升级，同时网络卫士安全网关采用双系统设计，在主系统发生故障时，用户可以在启动时选择 BACKUP 方式，用备份系统引导系统。

2.2 工作原理

2.2.1 处理数据流

一般来说，网络卫士安全网关的作用是控制外部的非信任网络（如 Internet）对内部信任网络的访问，以及内部网络中不同区域之间的相互访问。网络卫士安全网关所使用的 TOS 操作系统平台是基于模块设计的最新操作系统。通过加载防火墙模块、包过滤模块、深度过滤模块、乃至 VPN 模块、防病毒模块等一系列功能模块，网络卫士安全网关可以通过设置访问规则，并配合包过滤规则，以及接口属性等机制，控制穿越安全设备的数据

流。加载各个功能模块后，网络卫士安全网关处理数据包的基本过程可以分为以下几个基本步骤：

1. 快速转发

对于一个新接收的合法报文，网络卫士安全网关将首先查询会话表，判断该报文是否属于某个已经存在的会话。如果是，则根据会话表中所包含的会话处理信息，如匹配会话的访问规则和地址转换策略，快速处理此报文。如果不存在，则说明此报文属于一个新的会话，网络卫士安全网关将检索路由表，地址转换策略表和访问规则表，收集与此报文相关的处理策略，即进入下一步骤。

2. 接收处理

网络卫士安全网关将调用相关的功能模块对接收的数据包进行初步处理。调用的功能模块包括：

- IDS 模块。用来对数据包进行入侵过滤检测。如果接收的数据报文匹配 IDS 入侵规则，则判定为非法报文并丢弃。
- VPN 模块。如果接收的数据包属于某个 VPN 连接，网络卫士安全网关将调用 VPN 模块对报文进行解密。
- IP-MAC 绑定模块。如果接收的数据包头所包含的 IP 地址和 MAC 地址信息违反了 IP-MAC 绑定表中的规则，则丢弃数据包。

3. 规则匹配

在这一步，安全网关将调用其它的功能模块对通过接收处理的数据包进行一系列的规则匹配操作。调用的模块包括：

- 包过滤（PF）模块。包过滤模块不仅仅对数据包进行 2 层或 3 层的协议过滤，还进一步的检查数据包是否属于被允许通过的服务。
- 地址转换模块。地址转换策略描述了对接收的报文的处理方式，网络卫士安全网关支持 4 种地址转换策略：**直接转发**方式，即对报文不作任何处理，直接转发，这是网络卫士安全网关的缺省地址转换策略；**源地址转换**方式，网络卫士安全网关将把接收的报文的源 IP 地址（或端口）转换为预先设定的 IP 地址（或端口），然后转发被修改源地址的报文；**目的地址转换**方式，该方式下，网络卫士安全网关将把接收的报文的目的 IP 地址（或端口），通常为安全网关接口地址，转换为预先设置的 IP 地址或端口（真实的 IP 地址或端口），然后转发被修改目的地址的报文。**双向地址转换**方式，顾名思义，也就是同时转换数据包的源和目的地址（或端口）。地址转换策略的详细设置介绍，请参见[9.4 地址转换](#)。
- 访问控制模块。访问控制规则描述了安全网关能否允许符合相关条件的报文通过。安全网关接收到报文后，将按策略的编号顺序逐条匹配访问规则表中所设定规则，一旦寻找到完全匹配的规则，则按照该策略所规定的操作（允许或丢弃）

处理该报文。如果不存在可匹配的访问策略，则该报文将被转发到目的接口。网络卫士安全网关将根据目的接口所在区域的缺省属性（允许访问，或禁止访问），处理该报文。有关访问规则的设置方法，请参见[9.2.5添加规则](#)。

- 深度过滤（DPI）模块。用来对数据包进行内容过滤。目前支持的协议包括 HTTP、FTP、SMTP、POP3、IMAP、TELNET、RSH 以及 DNS。安全网关调用深度过滤模块对以上协议的数据包进行内容检测，凡包含有非法内容的数据包将被禁止通过安全网关。

4. 创建会话

对于一个不存在会话匹配的报文，网络卫士安全网关将根据以上步骤的报文处理信息，在会话表中创建一条新的记录，包括该报文的地址，源地址，路由，地址转换策略，访问规则等信息，此后接收的属于此会话的报文将根据会话表中的记录信息采用相应处理。

5. 路由前处理

对于发送的 VPN 报文，系统将对其进行封装。VPN 加密后的报文目的地址有可能改变。另外，如果在通信过程中，策略发生改变，安全网关将重新调用包过滤、访问控制和深度过滤模块对数据包进行策略匹配。

6. 路由查询

网络卫士安全网关将根据路由表或各个接口所学习的 MAC 地址表选择报文的转发接口。如果数据包经过了地址转换操作，那么安全网关将查询地址转换表以根据真实的地址进行路由。

数据处理流程图如下：

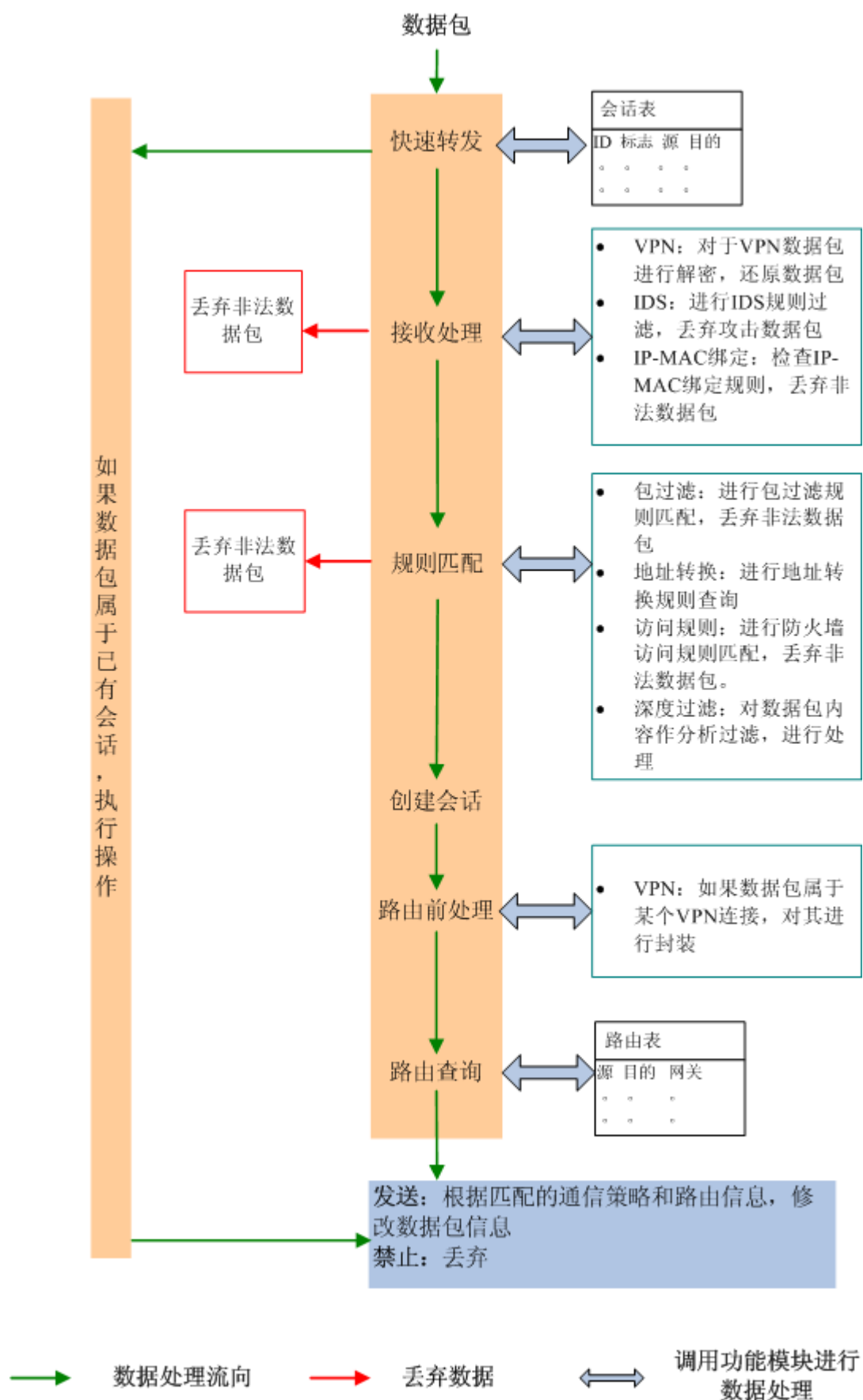


图 2-1 网络卫士安全网关数据包处理流程图

2.2.2 匹配访问控制规则

访问规则，是一组用户自定义的策略，这些规则可以描述满足哪些条件的报文可以通过网络卫士安全网关，以及满足哪些条件的报文将被网络卫士安全网关禁止。每一个访问策略中包含的信息主要包括：报文的源地址，目的地址，服务（协议类型和端口号），以及对满足条件的报文进行何种操作（转发或丢弃）。

在访问策略中，**策略源**定义了报文的来源，策略源可以是区域、地址（主机、子网、范围）、角色、VLAN等几类对象。当报文的源地址属于策略源的范围，则被认为满足策略源约束条件。**策略目的**定义了报文的目的地址范围，与策略源相同，可以包括一个或多个主机、子网、或范围，也可以包括多个区域（或VLAN）。**策略服务**定义了报文采用的网络协议或特定端口号。**访问控制**定义了网络卫士安全网关对满足策略的报文所采取的处理方式，包括允许（该报文被允许通过）和禁止（丢弃该包）。同时网络卫士安全网关支持用户定义访问策略有效的时段，即**访问时间**，即在哪一天或哪一时段访问策略有效。一个报文和某一条访问策略匹配指的是：报文的源地址包含于策略源定义、报文目的地址包含于策略目的，以及报文端口包含于策略服务，如果定义了访问时间，则报文的接收时间也必须满足策略访问时间约束。只有当一个报文完全符合策略中所规定的所有条件时，这条策略才匹配该报文。

需要特别说明的是，每条访问规则中可以定义一个内容过滤策略和一个应用程序识别策略，对应用层的内容进行过滤检测。网络卫士安全网关按照如下步骤查找匹配报文的访问策略。

网络卫士安全网关将按照访问策略的排列顺序检索访问控制规则表，逐一与数据包匹配。一旦发现匹配报文的访问策略，网络卫士安全网关将停止访问策略匹配检查，并根据最先匹配的那一条访问策略的规则定义，处理报文（允许或拒绝）。如没有任何访问策略能够匹配该报文，则按照网络卫士安全网关将根据发送接口的缺省访问控制属性，处理该报文。接口缺省属性的设置请参见[7.2设置区域](#)。

如果报文被禁止转发，则被丢弃；如果被允许转发，则查看该条策略中是否定义了DPI策略或应用程序识别策略。

如果策略中定义了DPI对象，则检查报文应用层的内容是否能匹配DPI中所包含的关键词。如果匹配，则按照该关键词的访问属性处理该报文。如不能匹配，则按照该DPI中定义的服务默认访问属性处理报文。访问属性分为3种：可读，可写，可执行。定义方法请参见[10内容过滤](#)。

网络卫士安全网关支持7种协议的深度过滤，用于控制整个受控网络内的内容过滤：HTTP、FTP、SMTP、POP3、IMAP、TELNET、以及RSH。

如果策略中定义了应用程序识别策略，则检查报文应用层是否使用了该应用程序识别策略中包含的协议。如果符合，则按照该应用程序识别策略规定的处理动作处理该报文。访问策略匹配过程如下所示。

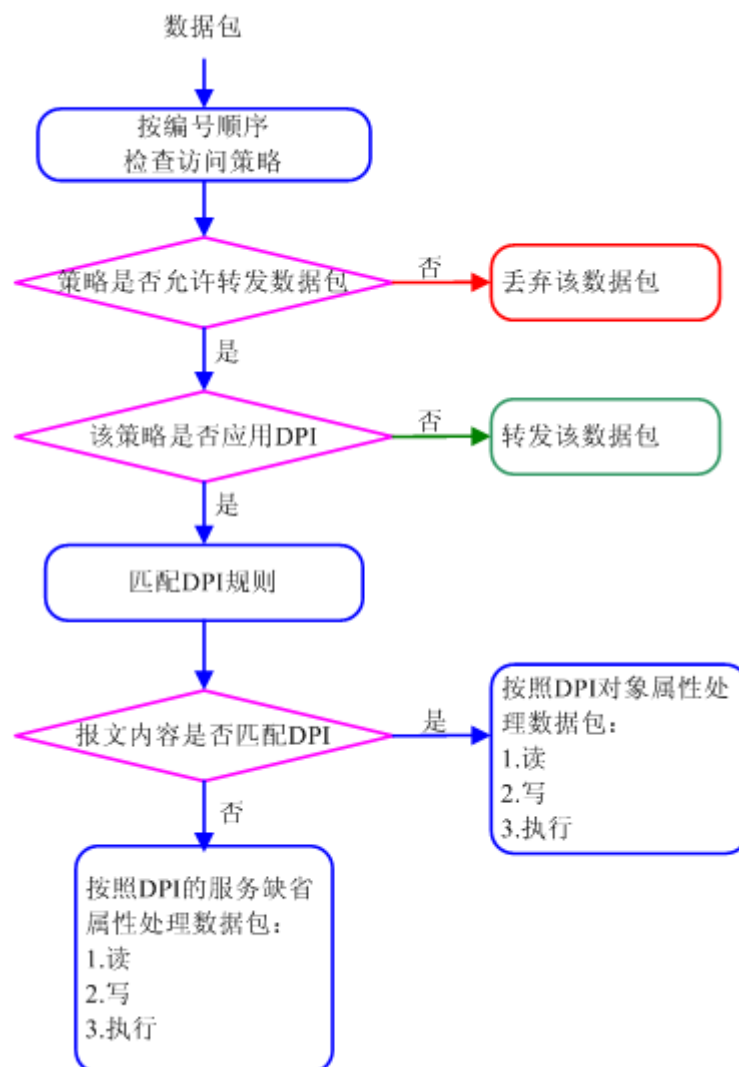


图 2-2 访问策略匹配流程图

2.3 工作模式

网络卫士安全网关可以在三种模式下工作：透明模式、路由模式以及混合模式。

2.3.1 路由模式

在这种模式下，网络卫士安全网关类似于一台路由器转发数据包，将接收到的数据包的源 MAC 地址替换为相应接口的 MAC 地址，然后转发。该模式适用于每个区域都不在同一个网段的情况。和路由器一样，网络卫士安全网关的每个接口均要根据区域规划配置 IP 地址。

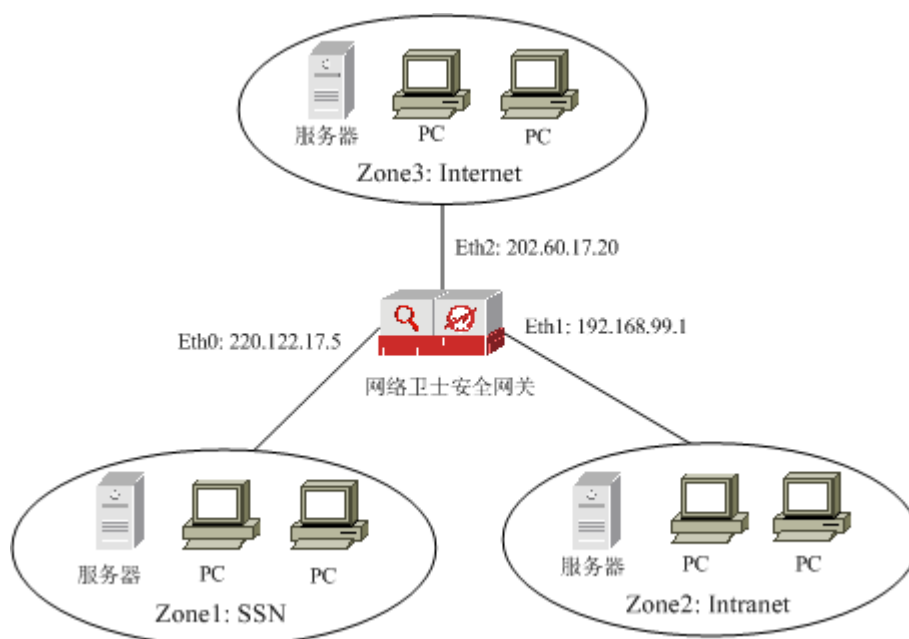


图 2-3 路由工作模式示意图

2.3.2 透明模式

在这种模式下，网络卫士安全网关的所有接口均作为交换接口工作。也就是说，对于同一 VLAN 的数据包在转发时不作任何改动，包括 IP 和 MAC 地址，直接把包转发出去。同时，网络卫士安全网关可以在设置了 IP 的 VLAN 之间进行路由转发。

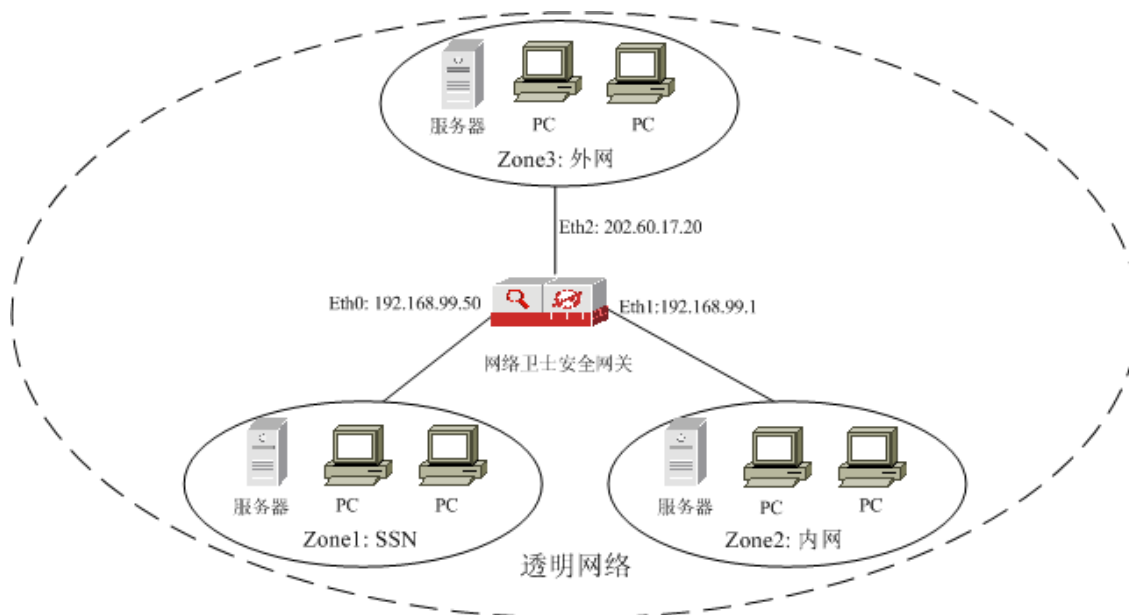


图 2-4 透明工作模式示意图

2.3.3 混合模式

顾名思义，这种模式是前两种模式的混合。也就是说某些区域（接口）工作在透明模式下，而其他的区域（接口）工作在路由模式下。该模式适用于较复杂的网络环境。如下图所示，Eth0 接口为路由接口，配置了 IP192.168.99.50，Eth0 属于区域 intranet；Eth1 和 Eth2 为交换接口，Eth1 属于 Internet 区域，Eth2 属于 SSN 区域，Eth1 和 Eth2 属于同一个 VLAN。

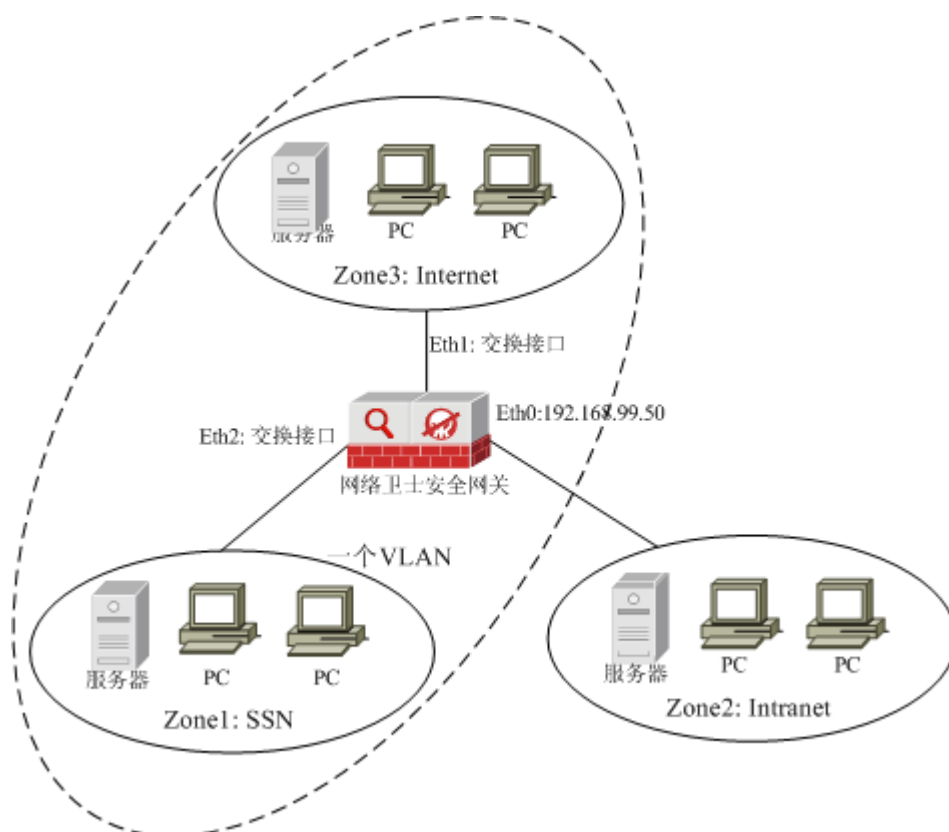


图 2-5 混合工作模式示意图

2.4 虚系统

网络卫士安全网关 v3.3 支持虚系统。所谓虚系统，就是在同一台设备的根系统上逻辑地划分出一套或多套相对独立的虚拟系统，每个虚拟系统都维护自己的配置，包括接口、对象、访问控制策略、NAT 策略等。这样，从逻辑上来看，一台网络卫士安全网关被分成了 2 台或多台独立的虚拟安全网关。某个虚拟系统的用户可以在安全网关上设置本虚系统的接口、对象、以及访问控制策略、包过滤策略和地址转换策略，就像配置一台独立的安全网关。网络卫士安全网关对虚系统的支持，满足了多个用户共用一台安全网关的需求。

需要说明的是，网络卫士安全网关的虚系统并不支持根系统的所有功能，如用户认证、VPN 等。

虚系统的创建和使用流程为：

- 1) 由根系统的超级管理员（superman）创建虚系统，并为每个虚系统分配接口、子接口、VLAN，具体操作方法请参见[6.2接口设置](#)和[6.3.2VLAN](#)。
- 2) 由根系统的超级管理员（superman）创建虚系统管理员。具体操作方法请参见[4.4配置系统管理员](#)。
- 3) 虚系统管理员登录安全网关，配置相应的虚系统。虚系统管理员登录和配置安全网关的方法与根系统管理员一样，可参见本手册的相关章节。

3 安全网关初始配置和管理方式

本章面向初次接触使用网络卫士安全网关的用户，主要介绍网络卫士安全网关外观、出厂配置以及管理网络卫士安全网关的几种方式。初步介绍了如何通过命令行和 WEBUI 管理中心对网络卫士安全网关进行简单管理。并介绍了对象的概念以及对象在网络卫士安全网关配置管理中的作用。

本章内容主要包括：

- 网络卫士安全网关的出厂配置：介绍网络卫士安全网关出厂时的缺省配置，如接口、用户类型等。
- 网络卫士安全网关的工作状态：通过指示灯介绍，帮助用户了解网络卫士安全网关的工作状态。
- 网络卫士安全网关的管理方式：介绍安全网关管理方式，包括本地管理（通过 Console 口管理）和远程管理（通过 WEBUI 方式管理安全网关）。
- 设置对象。引入了对象这个概念，并详细介绍了如何设置对象。

3.1 出厂配置

产品出厂配置包括缺省管理用户、缺省空闲超时、缺省系统参数、缺省日志服务器、缺省接口配置、缺省地址对象、缺省区域对象和访问控制规则。用户可根据实际环境更改出厂配置，具体操作请参照相关章节。

3.1.1 缺省管理用户

网络卫士安全网关出厂默认的管理用户：superman，密码 talent。

3.1.2 缺省空闲超时

为保证网络卫士安全网关的安全性，系统设置了空闲超时。当用户使用命令行对网络卫士安全网关进行管理（包括 CONSOLE 口本地管理、SSH 远程管理、TELNET 远程管理），或使用 WEBUI 界面远程管理安全网关时，如果 3 分钟内无任何操作，系统将退出至登录界面。

3.1.3 缺省系统参数

项目	缺省值

项目	缺省值
最大登录失败次数	5
最大并发管理数	5
同一用户最大并发管理数	5

3.1.4 缺省日志服务器

服务器地址	连接接口	所用端口号	日志类型	传输
192.168.1.253	eth0	UDP:514	syslog	禁止传输

3.1.5 缺省接口配置

接口名称	IP	MASK
eth0 (MGMT)	192.168.1.254	255.255.255.0
eth1 (HA)	无	无

3.1.6 缺省地址对象

对象名称	对象类型	定义范围
ANY	地址段	0.0.0.0 — 255.255.255.255

3.1.7 缺省区域对象

对象名称	对象类型	绑定接口
area_eth0	区域	eth0

3.1.8 本机服务访问控制规则

规则名称	作用	开放接口	允许对象
Webui	通过浏览器管理安全网关	eth0	ANY
SSH	通过 SSH 管理安全网关	eth0	ANY
Update	升级安全网关	eth0	ANY
PING	PING 安全网关	eth0	ANY
GUI	通过设备管理器管理安全网关	eth0	ANY

3.2 工作状态

网络卫士安全网关的硬件设备安装完成之后，就可以上电了。在工作过程中，用户可以根据网络卫士安全网关面板上的指示灯来判断安全网关的工作状态，具体请见下表：

指示灯名称	指示灯状态描述
工作灯（Run）	当安全网关进入工作状态时，工作灯闪烁。
主从灯（M/S）	主从灯亮的时候，代表这台网关是工作端；反之，如果主从灯处于熄灭状态，则该安全网关工作在备份模式。
管理灯（MGMT）	当网络管理员，如安全审计管理员，登录安全网关时，管理灯点亮。
日志灯（Log）	当有日志记录动作发生时，且前后两次日志记录发生的时间间隔超过 1 秒钟时，日志灯会点亮。

说明

- ✧ 管理员类型请参见[4.4.2配置管理权限](#)。
- ✧ 不同型号的网络卫士安全网关的指示灯可能会有区别。

3.3 管理方式

网络管理员可通过多种方式管理网络卫士安全网关。包括通过 CONSOLE 口进行本地管理以及通过以下几种方式进行远程管理：

- WEBUI 方式（通过浏览器直接登录安全网关进行管理）
- SSH（Secure Shell）
- TELNET

第一次使用网络卫士安全网关，管理员可以通过 CONSOLE 口以命令行方式、通过浏览器以 WEBUI 方式进行配置和管理。在下面几节中，将会介绍如何通过 CONSOLE 口登录到网络卫士安全网关并配置其他几种管理方式。本手册将主要介绍如何通过 WEBUI 方式对安全网关进行管理。

3.3.1 通过 CONSOLE 口管理网络卫士安全网关

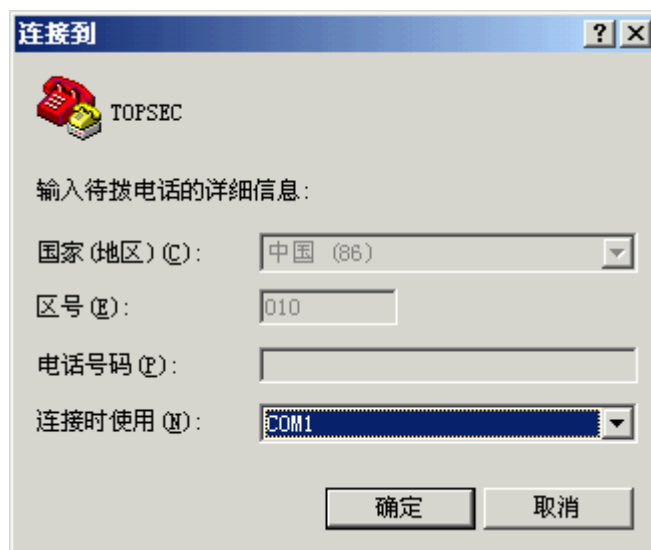
通过 CONSOLE 口登录到网络卫士安全网关，可以对安全网关进行一些基本的设置。用户在初次使用安全网关时，通常都会登录到安全网关更改出厂配置（接口、IP 地址等），使在不改变现有网络结构的情况下将安全网关接入网络中。这里将详细介绍如何通过 CONSOLE 口连接到网络卫士安全网关：

1) 使用一条串口线（包含在出厂配件中），分别连接计算机的串口（这里假设使用 com1）和安全网关的 CONSOLE 口。

2) 选择 开始 > 程序 > 附件 > 通讯 > 超级终端，系统提示输入新建连接的名称。



3) 输入名称，这里假设名称为“TOPSEC”，点击“确定”后，提示选择使用的接口（假设使用 com1）。



4) 设置 com1 口的属性，按照以下参数进行设置。

参数名称	取值
每秒位数:	9600
数据位:	8
奇偶校验:	无
停止位:	1

5) 成功连接到安全网关后，超级终端界面会出现输入用户名/密码的提示，如下图。



6) 输入系统默认的用户名: superman 和密码: talent, 即可登录到网络卫士安全网关。
登录后, 用户就可使用命令行方式对网络卫士安全网关进行配置管理。

说明

- ◇ 网络卫士安全网关对于用户名和密码是大小写敏感。
- ◇ 本地管理员具有安全网关所有管理权限, 为超级管理员。
- ◇ 关于如何通过命令行配置安全网关, 请参考《TopGate 命令行手册——基础配置》。

3.3.2 设置其他管理方式

从 CONSOLE 口本地登录网络卫士安全网关后, 管理员可以通过命令行对安全网关进行一些必要的设置, 如更改、添加接口 IP, 添加其他的远程管理方式 (包括 “WEBUI 管理”、“SSH” 等), 方便对网络卫士安全网关的管理维护。

本节将介绍如何使用命令行方式添加其它管理方式。另外, 管理员还可以使用浏览器通过 Eth0 (或 MGMT) 接口对安全网关进行设置。这要求管理主机与 Eth0 (或 MGMT) 的缺省出厂 IP 处于同一网段。

3.3.2.1 设置接口 IP 地址

用户可通过网络卫士安全网关的任一物理接口远程管理网络卫士安全网关, 但是在此之前, 管理员必须为此物理接口配置 IP 地址, 作为远程管理网络卫士安全网关的管理地址。命令行语法如下:

network interface <string> ip add <ipaddress> mask <netmask>

参数说明:

string: 网络卫士安全网关物理接口名称, 字符串, 例如 eth0。

ipaddress: IP地址, 如192.168.91.22。

netmask: 子网掩码, 如255.255.255.0。

3.3.2.2 定义地址对象

管理员应定义允许远程管理网络卫士防安全网关防火墙的IP地址范围, 可以是某一特定的IP地址, 也可以来自某一子网、地址范围或地址组。在命令行中使用**define host/define subnet/define range/define group_address** 这几个命令定义IP地址、子网、地址范围或地址组。命令行语法如下:

定义IP: **define host add name** <string> **ipaddr** <ipaddress>

定义子网: **define subnet add name** <string> **ipaddr** <ipaddress> **mask** <netmask>

定义地址范围: **define range add name** <string> **ip1** <ipaddress> **ip2** <ipaddress>

定义地址组: **define group_address add name** <string> **member** <string>

参数说明:

string: 对象名称, 字符串。

ipaddress: IP地址, 如192.168.91.22。

netmask: 子网掩码, 如255.255.255.0。

成功定义后系统会自动为已定义的 IP 地址、子网、地址范围或地址组生成对应的 ID 号。查看用户已定义的对象 ID 号命令行语法如下:

查看已定义的所有IP地址对象: **define host show**

查看已定义的所有子网对象: **define subnet show**

查看已定义的所有地址范围对象: **define range show**

查看已定义的所有地址组对象: **define group_address show**

3.3.2.3 指定管理方式

管理员可以为已定义的 IP 地址 (或子网、地址段) 指定其可使用的远程管理方式。在命令行中可以使用 **pf service** 命令指定管理方式。命令行格式如下:

pf service add name <gui| monitor|ping|telnet|tosids|auth|cgi_auth| update | webui| ipsecvpn | l2tp| ntp| pptp| rip|snmp|ssh|dhcp| sslvpn|bgp| sslvpnmgr|websv> **area** <string> <[addressid <number>]| [addressname <string>]>

相关参数说明:

参数	说明
add	增加一条服务访问规则
name	选择 TOS 设备开放的服务名
GUI	允许用户通过网络卫士安全网关管理器对设备进行配置和管理。

参数	说明
WEBUI	当安全网关不包含 SSL VPN 模块时，开放该服务用于允许用户通过 WEBUI 的 443 端口对设备进行配置和管理。 当安全网关包含 SSL VPN 模块时，要实现管理员通过 WEBUI 对设备进行管理无需开放该服务，只需开放 SSLVPNMG 服务。要实现普通用户通过 443 端口访问设备时只需开放 SSLVPN 服务。
AUTH	允许用户使用安全网关设备所提供的认证机制。
CGI_AUTH	允许 CGI 认证用户使用安全网关设备所提供的认证机制。
UPDATE	允许用户通过 TOPSEC 管理中心对设备进行远程升级。
MONITOR	允许用户根据其设定的条件监控设备的运行状态。
SNMP	允许设备与 SNMP 管理主机进行通信。
PING	允许用户可以 PING 到设备的物理接口地址、VLAN 虚接口和子接口的地址。
SSH	允许用户通过 SSH 方式对设备进行配置和管理。
TELNET	允许用户通过 TELNET 对设备进行配置和管理。
TOSIDS	允许与 IDS 设备间的联动。
DHCP	允许设备作为 DHCP 服务器、DHCP 客户端或 DHCP 中继使用。
IPSecVPN	允许设备与 VPN 设备建立 IPSec VPN 隧道进行通信。
RIP	允许使用 RIP 动态路由协议。
L2TP	允许 L2TP 客户端登录。
PPTP	允许 PPTP 客户端登录。
NTP	允许系统使用 NTP 协议保持设备本身和其他设备的时钟同步。
SSLVPN	当安全网关包含 SSL VPN 模块时，才包含该选项，用于开放 443 和 4430 端口，允许使用 SSLVPN 的相关功能，包括全网接入、普通用户登录网关等。
SSLVPNMG	当安全网关包含 SSL VPN 模块时，才包含该选项，用于管理员通过 8080 端口对安全网关进行管理。
BGP	允许使用 BGP 动态路由协议。
WEBSV	开放 WEBSV 服务
area	选择允许服务请求来自哪个区域，只能从现有区域中选择一个
string	网络卫士安全网关网络区域名称（字符串）
addressid	设定允许客户地址对象 ID 号
number	数值，必须是已经定义的主机、子网或范围地址对象的 ID 号
addressname	设定允许客户地址对象名称
string	字符串，必须是已经定义的主机、子网或范围地址对象名

3.3.2.4 设置管理方式实例

下面是个简单的配置实例，用以说明如何设置网络卫士安全网关的 WebUI 管理方式：

1. 为网络卫士安全网关的物理接口 Eth1 配置 IP 地址 192.168.91.88，子网掩码是 255.255.255.0，此地址将作为网络卫士安全网关的管理地址：

进入 network 组件	topsecos# network
配置 Eth1 接口 IP	topsecos.network# interface eth1 ip add 192.168.91.88 mask

	255.255.255.0

2. 定义一个 area 对象 “webui-area”，并设置其属性为 eth1:

进入 define 组件	topsecos.network# exit topsecos# define
配置 Eth1 接口 IP	topsecos.define# area add name webui-area attribute eth1

3. 定义一个 IP 地址对象 “manage-host”，地址是 192.168.91.250，此地址是被允许的远程管理网络卫士安全网关的地址:

保持 define 组件	topsecos.define#
定义管理主机对象	topsecos.define# host add name manage-host ipaddr 192.168.91.250

4. 设置从 192.168.91.250 这个 IP 可以浏览器远程管理该安全网关:

进入 pf 组件	topsecos.define# exit topsecos# pf
设置开放服务规则	1) 当安全网关不包含 SSL VPN 模块时，开放 WEBUI 服务即可，用于管理员通过 443 端口对安全网关进行管理。 topsecos.pf# service add name webui area webui-area ddressname manage-host 2) 当安全网关包含 SSL VPN 模块时，开放 SSLVPNMgr 服务即可，用于管理员通过 8080 端口对安全网关进行管理。 opsecos.pf# service add name sslvpnmgr area webui-area ddressname manage-host

3.3.3 管理主机的相关设置

在网络卫士防安全网关上成功添加管理方式后，还需要在管理主机进行必要设置才能远程管理安全网关。下面简要说明了不同管理方式的管理主机的要求:

SSH，需要 SSH 软件，如 PUTTY 等，需要设置连接地址为网络卫士安全网关管理地址;

WEBUI，需要在管理主机安装浏览器，并进行必要的配置。

说明

- ◇ 管理主机的浏览器需支持 SSLv2.0、SSLv3.0 或 TLSv1.0 协议中的任意一种。
- ◇ 网络卫士安全网关支持 IE5.0, IE6.0, Mozilla firefox 1.0.2, Mozilla firefox1.0.3, Mozilla firefox 1.0.4, Mozilla firefox 1.0.5, Netscape7.1 (只能在 Linux9.0 中支持), Netscape8.0 (支持 Linux9.和 Linux10.0), Opera8.0(只支持 Windows2000 Professional, Windows2000 Server)。
- ◇ 使用前需确认浏览器选项中 cookie 相关选项打开。

3.4 通过浏览器登录安全网关

管理员在管理主机的浏览器上输入安全网关的管理URL，例如：<https://192.168.1.254>，（如果包含SSL VPN模块，则URL应当为<https://192.168.1.254:8080>），弹出如下的登录页面。



输入用户名密码（网络卫士安全网关默认出厂用户名/密码为：[superman/talent](#)）后，点击“登录”，就可以进入管理页面。

说明

- ✧ 在输入URL时要注意以“https://”作为协议类型，例如<https://192.168.1.254>。
- ✧ 网络卫士安全网关对于用户名和密码大小写敏感。

3.5 初始配置向导

管理员通过WEBUI登录设备后，系统为管理员提供了使用配置向导对设备配置进行简单配置的功能。在WEBUI界面右上方的菜单栏选择 **初装向导**，进入配置向导页面，如下图所示。

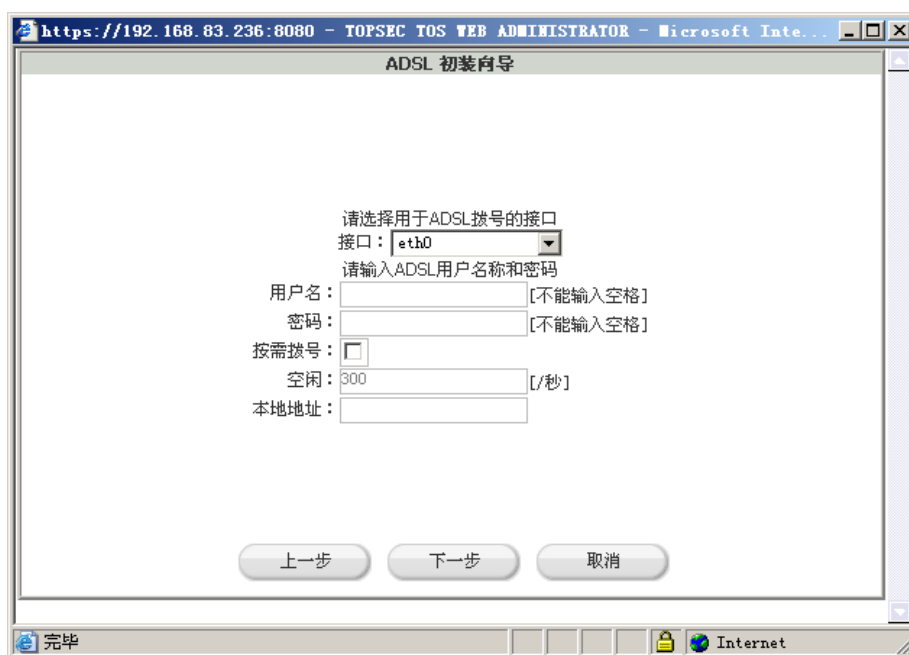


通过初装向导，管理员可以对其进行简单配置（包括 ADSL 拨号设置和专线接入设置），以便企业通过该设备接入外网（如 Internet）。

3.5.1 ADSL 配置向导

ADSL 配置向导用于配置 ADSL 拨号参数，以便该设备通过 ADSL 拨号方式（外网口的 IP 为动态 IP）与外网建立通信链路。

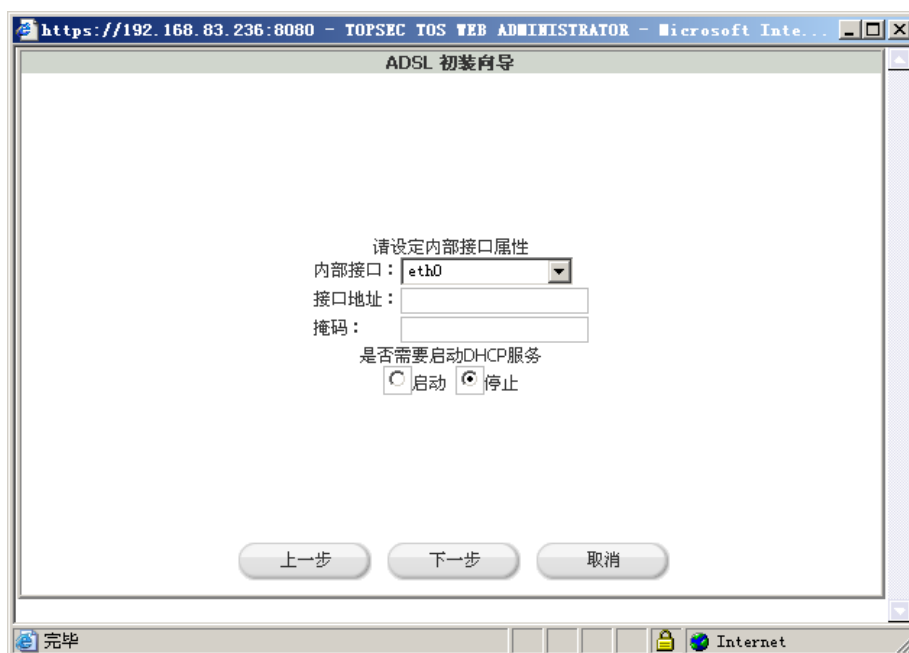
1) 在上图中勾选“ADSL 初装向导”右侧的单选按钮，然后点击“下一步”按钮，界面如下图所示：



窗口中的参数说明如下表所示。

参数	说明
接口	选择与 ADSL Modem 绑定的在线设备的以太网接口。 说明：ADSL 拨号设置成功后，该接口与在线设备的 ADSL 属性进行绑定。
用户名	设置 ADSL 拨号时需要的用户名，最多为 31 个字符。 说明：该用户名由电话局提供。
密码	设置 ADSL 拨号时需要的用户密码，最多为 31 个字符。 说明：该用户密码由电话局提供。
按需拨号	指是否选择按需拨号方式。如果选中了“按需拨号”后面的复选框，那么当有流量通过安全网关与 ADSL Modem 绑定的安全网关以太网接口时，系统会自动拨号。否则，需要点击“开始拨号”按钮才开始建立内外网之间的通信链路。
空闲	如果选中了“按需拨号”后面的复选框，则管理员可以在“空闲”处修改 ADSL 链路空闲时间，默认为 300 秒。
本地地址	如果 ADSL 服务提供商支持给 ADSL 用户分配静态 IP 地址，则在本选项处需要输入此 IP 地址；否则为空即可。

2) 参数设置完成后，点击“下一步”按钮，进入内部接口信息设置界面，如下图所示。

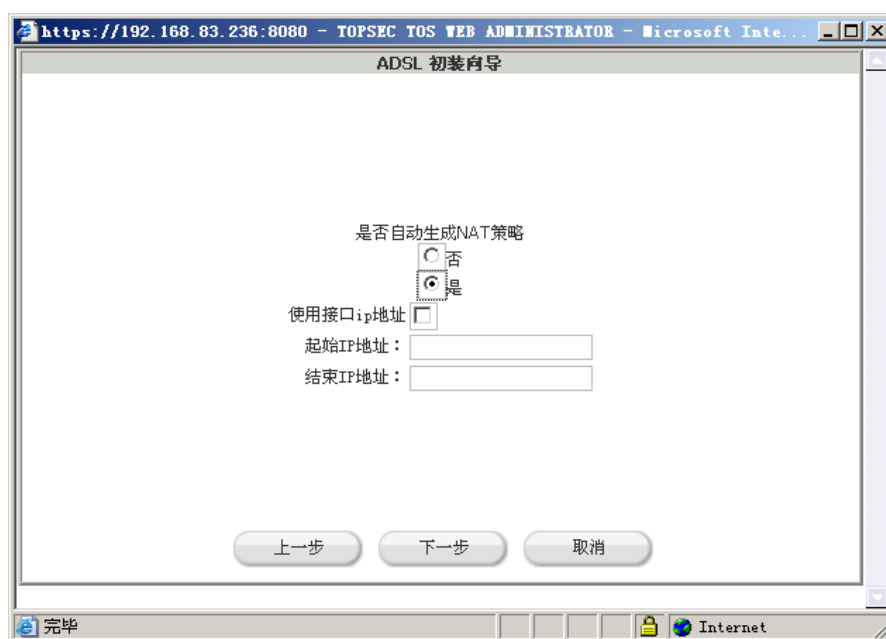


窗口中的参数说明如下表所示。

参数	说明
内部接口	选择与企业内网相连的在线设备的接口。
接口地址	设置该内部接口的 IP 地址。 说明：如果在线设备的默认出厂配置中配置了该内部接口的 IP 地址，则将被此处配置的 IP 地址覆盖。
掩码	设置该内部接口 IP 的子网掩码。
是否需要启动	选择是否启动内部接口的 DHCP 服务。

参数	说明
DHCP 服务	选中“启动”后，可以在该设备的内部接口上启动 DHCP Server 服务，以便该在线设备作为 DHCP 服务器为内网接口所在子网的主机动态分配 IP 地址。 说明：在设备中使用内部接口的 DHCP 服务之前，还需要开放该接口所属区域的 DHCP 服务，具体操作请参见 4.2.2.2 开放服务。
子网/掩码	设置为哪个子网创建 DHCP 作用域。 说明：只有选中了“启动” DHCP Server 服务，才能设置该参数值。
分配起始地址/分配终止地址	输入 DHCP 服务器可以为客户端分配地址的范围。应当与“子网”设定的 IP 在同一个网段，并且不能包含已经分配的 IP 地址。 说明：只有选中了“启动” DHCP Server 服务，才能设置该参数值。
DNS	可选项，如果 DHCP 服务器设定了 DNS 服务器地址，则客户端主机在获取 IP 地址的同时按照该设置设定 DNS 服务器地址。 说明：只有选中了“启动” DHCP Server 服务，才能设置该参数值。
网关地址	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定其网关地址。 说明：只有选中了“启动” DHCP Server 服务，才能设置该参数值。

3) 参数设置完成后，点击“下一步”按钮，进入“自动生成 NAT 策略”窗口，如下图所示。

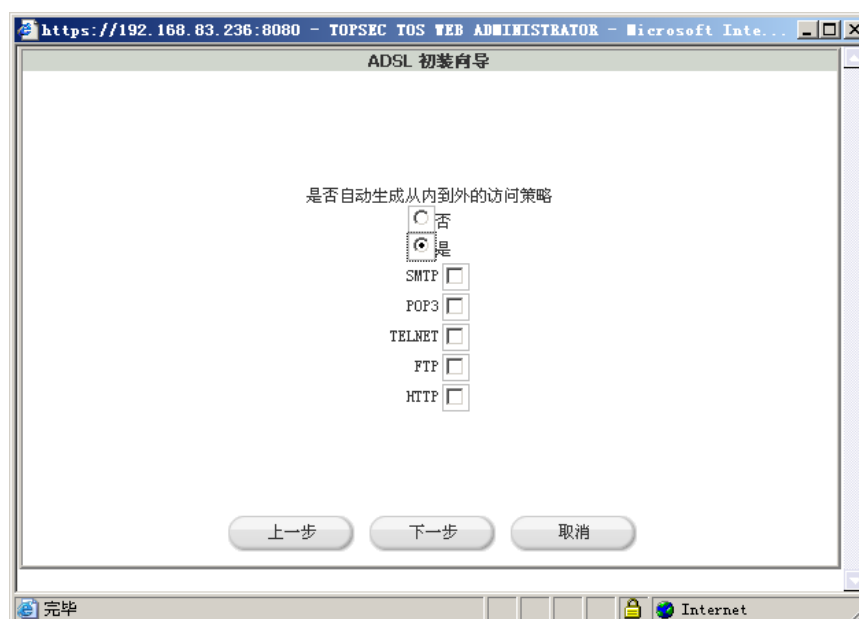


窗口中的参数说明如下表所示。

参数	说明
是否自动生成 NAT 策略	选择是否自动生成 NAT 策略。
使用接口 IP 地址	选中“使用接口地址”后，在线设备中将自动生成一条源 NAT 策略：源为“any”，目的为“any”。 说明：只有在“自动生成 NAT 策略”中选中了“是”左侧的单选按钮，才能够配置该参数。

参数	说明
起始 IP 地址/终止 IP 地址	配置了起始 IP 地址和终止 IP 地址后，在线设备中将首先自动生成一个地址范围对象（名称为 adsl_addrgroup），然后自动生成一条源 NAT 策略：源为“any”，目的为“any”。 说明：只有在“自动生成 NAT 策略”中选中了“是”左侧的单选按钮，并且没有选中“使用接口 ip 地址”才能够配置该参数。

4) 参数配置完成后，点击“下一步”按钮，进入“自动生成从内到外的访问控制策略”，如下图所示。



窗口中的参数说明如下表所示。

参数	说明
自动生成从内到外的访问控制策略	选择是否为该在线设备自动生成从内到外的访问控制策略。
SMTP/ POP3/ TELNET / FTP / HTTP	选择是否为 HTTP、SMTP、FTP、POP3 或 TELNET 服务自动生成从内到外的访问控制策略。 说明：1) 只有选择了自动生成从内到外的访问控制策略，才能够配置该参数。2) 默认情况下，自动生成一条访问控制策略禁止所有服务（源为“any”，目的为“any”，访问权限为“禁止”）；当选中某些服务后，将在该禁止策略上方增加一条允许这些服务的访问控制策略（源为“any”，目的为“any”，服务为选中的这些服务，访问权限为“允许”）。

5) 参数设置完成后，点击“下一步”按钮，进入是否需要阻断冲击波、振荡波端口设定界面，如下图所示。



选择“是”，则可以在该在线设备中添加一系列的报文阻断策略，以便阻断所有通过该设备的冲击波和振荡波病毒。

6) 参数设置完成后，点击“下一步”按钮，设置是否修改管理员密码，如下图所示。



当选择“是”后，可以输入管理员的新密码，并再次输入确认密码。

7) 点击“确定”按钮，进入“完成 ADSL 配置”窗口，如下图所示。



8) 点击“完成”按钮，在弹出的如下图所示对话框中点击“确定”按钮，退出 ADSL 初始化配置界面，并按照初装配置对设备进行初始化。



3.5.2 固定 IP 配置向导

“固定 IP 配置向导”用于配置专线接入参数，以便该设备通过专线方式（外网口的 IP 为固定 IP）与外网建立通信链路。

1) 在WEBUI界面右上方的菜单栏选择 **初装向导**，进入配置向导页面，如下图所示。



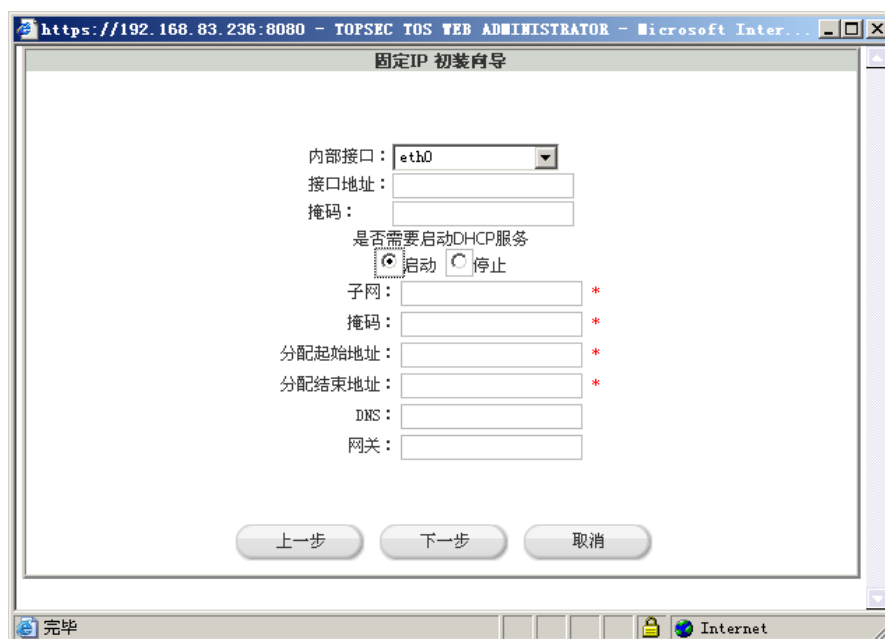
2) 勾选“固定 IP 初装向导”右侧的单选按钮，并点击“下一步”，进入“专线外部接口配置”界面，如下图所示。



窗口中的参数说明如下表所示。

参数	说明
外部接口	选择与外网连接的在线设备的以太网接口。
接口地址	配置该外部接口的 IP 地址。
掩码	配置该外部接口 IP 的子网掩码。
缺省网关	配置该外部接口的缺省网关 IP。

3) 参数配置完成后，点击“下一步”按钮，进入“专线内部接口设置”窗口，如下图所示。



窗口中的参数说明如下表所示。

参数	说明
内部接口	选择在线设备的内部接口。
接口地址	配置该内部接口的 IP 地址。
掩码	配置该内部接口 IP 的子网掩码。
是否需要启动 DHCP 服务	选择是否启动内部接口的 DHCP 服务，默认为停止状态。 选中“启动”后，可以在该在线设备的内部接口上启动 DHCPServer 服务，以便该在线设备作为 DHCP 服务器为内网接口所在子网的主机动态分配 IP 地址。 说明：在设备中使用内部接口的DHCP服务之前，还需要开放该接口所属区域的DHCP服务，具体操作请参见 4.2.2.2开放服务 。
子网/掩码	设置为哪个子网创建 DHCP 作用域。 说明：只有选中了“启动”DHCPServer 服务，才能设置该参数值。
分配起始地址/分配终止地址	输入 DHCP 服务器可以为客户端分配地址的范围。应当与“子网”设定的 IP 在同一个网段，并且不能包含已经分配的 IP 地址。 说明：只有选中了“启动”DHCPServer 服务，才能设置该参数值。
DNS	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定 DNS 服务器地址。
网关	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定其网关地址。

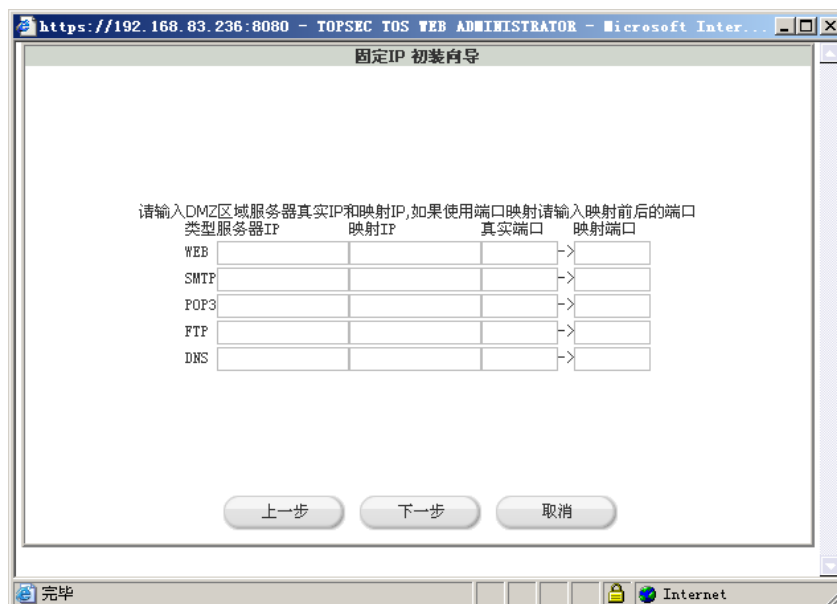
4) 参数配置完成后，点击“下一步”按钮，进入“专线 DMZ 配置”窗口，如下图所示。



窗口中的参数说明如下表所示。

参数	说明
DMZ 接口	选择在线设备的 DMZ 接口。
接口地址	配置该 DMZ 接口的 IP 地址。
掩码	配置该 DMZ 接口 IP 的子网掩码。

5) 参数配置完成后, 点击“下一步”按钮, 进入“专线 DMZ 服务映射设置”窗口, 如下图所示。



窗口中的参数说明如下表所示。

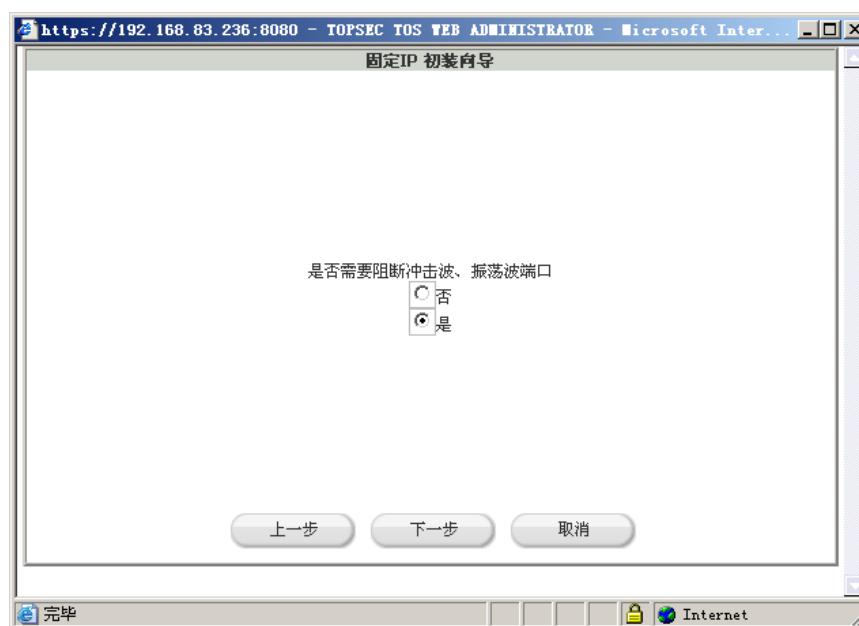
参数	说明

参数	说明
服务器 IP	配置 DMZ 区域中服务器的 IP 地址。
映射 IP	配置外部访问服务器时的访问 IP。
真实端口	配置 DMZ 区域中服务器开放的应用端口。
映射端口	配置外部访问服务器时的访问端口。

说明

- 配置成功后，对于每个专线 DMZ 服务映射设置，在线设备中都将首先自动生成两个主机地址对象（分别对应“服务器 IP”和“映射 IP”）和两个自定义服务对象（分别对应“真实端口”和“映射端口”），然后自动生成一条目的 NAT 策略：源为“any”，目的为与“映射 IP”对应的主机地址对象，服务为与“映射端口”对应的自定义服务对象，转换后的目的地址为与“服务器 IP”对应的主机地址对象，转换后的目的端口为与“真实端口”对应的自定义服务对象。

6) 参数设置完成后，点击“下一步”按钮，进入“是否阻断冲击波、振荡波端口”窗口，如下图所示。



在窗口中选择是否阻断冲击波、振荡波端口。

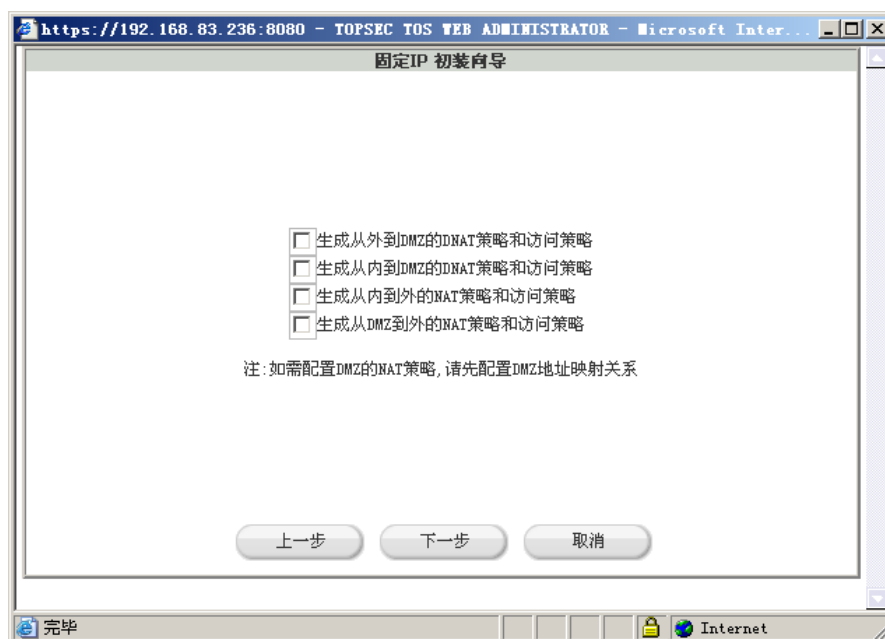
选中“阻断冲击波、振荡波端口”左侧的复选框后，可以在该在线设备中添加一系列的报文阻断策略，以便阻断所有通过该设备的冲击波和振荡波病毒。

7) 参数设置完成后，点击“下一步”按钮，进入“修改管理员密码”窗口，如下图所示。



选择“是”，则可以在下面输入管理员的新密码，并再次输入确认密码。

8) 参数设置完成后，点击“下一步”按钮，进入 NAT 策略和访问控制策略设置窗口，如下图所示。



管理员可以选择相应选项，则在设备中将直接生成相应的 NAT 策略及访问控制规则，保证内网用户能够通过专线方式与外网建立通信链路。

9) 点击“下一步”完成专线配置，窗口中可以查看配置信息，如下图所示。



10) 如果配置无误，选择“完成”按钮，弹出确认提示框，如下图所示。



11) 点击“确定”按钮即可退出初始化配置界面，并按照设置对系统进行初始化。

4 系统管理

系统管理主要包括：查看基本信息，查看设备运行信息，配置系统信息、配置维护信息、配置系统管理员等。

4.1 基本信息

系统的基本信息包括系统状态、设备的接口信息、各个功能模块的许可证信息、系统资源占用情况，以及设备接收到的警告信息窗口等等。

1) 选择 **系统管理 > 基本信息**，在右侧界面中可以查看当前设备的基本信息，如下图所示。



默认情况下显示“系统状态”窗口、“接口信息”窗口、“安全引擎信息”窗口、“警告信息”窗口、“系统资源”窗口和“病毒排行榜”窗口。

具体显示哪些窗口由设备的 license 来控制，当设备不包含某模块时，不会有模块相关的基本信息窗口。

a) “系统状态”窗口显示各个信息说明如下表：

参数	说明
产品型号	显示该设备所对应的产品型号。
序列号	显示唯一标识设备的序列号信息。
持续运行时间	显示开机到目前为止设备的持续运行时间。
系统日期	显示安全网关系统内置时钟的当前日期，管理员可以点击“更改”按钮，跳转至“系统时间设置”模块修改系统时间。具体请参见 4.2.3设置系统时间 。
高可用性	显示是否启用了双机热备功能，管理员可以点击“配置”按钮，跳转至“双机热备”模块进行相关设置。具体请参见 16.2高可用性 。
设备名	设定安全网关的系统名称，默认为 TopsecOS，在用户使用命令行时，初次使用或管理员未配置时，命令提示符显示为“TopsecOS#”。管理员可以点击“更改”按钮修改设备名称。
软件版本	显示设备当前的软件版本号。管理员可以点击“升级”按钮，跳转至“系统升级”界面对设备进行升级。具体请参见 4.3.2系统升级 。

b) “接口信息”窗口处可以查看设备的所有物理接口的名称、工作模式、接口地址、协商模式、工作速率以及接口是否启用等信息。

点击具体的接口名称时，管理员在弹出的窗口中可以查看到当前接口的流量统计情况，如下图所示。查看完毕，需要管理员点击“✕”图标关闭该窗口。



The screenshot shows a window titled "接口信息" (Interface Information). It lists several network interfaces. The first interface, "eth0", is selected and highlighted in green. Below the interface list, a detailed traffic statistics table is displayed for the selected interface.

统计内容	统计值
interface eth0 receive packets	28109
receive bytes	2866943
tcp receive packets	15308
tcp receive bytes	2077575
udp receive packets	3055
udp receive bytes	279900
icmp receive packets	672
icmp receive bytes	80703
transmit packets	20428
transmit bytes	3671284
input rate	9497 bps
output rate	16830 bps

c) “安全引擎信息”窗口如下图所示。

安全引擎信息	
系统许可证版本	001[升级]
防病毒许可证	无许可证[升级]
防病毒特征库版本	[升级]
IPS规则库	2009.11.20[升级]
应用识别规则库版本	2009.11.23[升级]
VPN版本	IV-6-3-6-100518
VRC最大用户数	1000
SSL VPN版本	SV-2.0-058e-100519
SSLVPN最大用户数	5

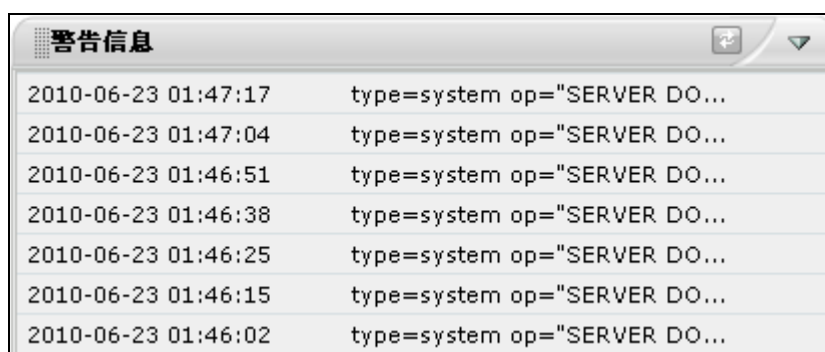
各个信息说明如下表：

参数	说明
系统许可证版本	显示设备许可证文件的版本号信息。管理员可以点击“升级”按钮，跳转至“许可证升级”界面对设备许可证进行升级。 说明： 网络卫士安全网关通过许可证文件来表明当前设备中能够使用的模块以及各项性能指标，许可证文件只能针对特定设备，而且只能使用一次。客户可以通过购买的方式对现有的功能进行扩充，性能进行升级。许可证版本号表明设备中许可证文件的版本号，每升级一次，版本号自动加一。
防病毒许可证	显示病毒库的许可证文件的更新时间。管理员可以点击“升级”按钮，跳转至“防病毒许可证升级”界面对设备的防病毒许可证进行升级。 说明： 天融信网络安全设备的病毒库是有使用期限的，其许可证到期后，必须通过更新许可证文件的方法获得授权，进而继续使用并及时更新病毒库。管理员可以点击“升级”按钮，对许可证文件进行更新。具体请参见《TopGate 管理手册——防病毒配置》手册的相关说明。
防病毒特征库版本	显示病毒库的最新更新时间。管理员可以点击“升级”按钮，跳转至“病毒库升级”界面对设备的病毒库进行升级。 说明： 天融信网络安全设备是根据病毒库来查杀病毒的，所以为了使病毒库保持最新的状态，管理员可以在此点击“升级”按钮，系统跳转至病毒库升级界面，对病毒库进行升级。具体请参见《TopGate 管理手册——防病毒配置》手册的相关说明。
IPS 规则库	显示 IPS 规则库的最新更新时间。管理员可以点击“升级”按钮，跳转至“规则库更新”界面对设备的 IPS 规则库进行升级。 说明： 天融信网络安全设备是根据 IPS 规则库来进行攻击检测，因此需要定期升级来保证设备对入侵的防御能力。

参数	说明
应用识别规则库版本	显示应用识别库的最新更新时间。管理员可以点击“升级”按钮，跳转至“应用识别规则库升级”界面对设备的应用识别库进行升级。 说明： 天融信网络安全设备根据应用识别规则库来进行应用程序识别。
VPN 版本	显示当前设备中 IPSec VPN 引擎的版本号信息。
VRC 最大用户数	显示当前设备允许同时登录设备的 VRC 用户的最大数值。
SSL VPN 版本	显示当前设备中 SSL VPN 引擎的版本号信息。
SSL VPN 最大用户数	显示当前设备允许同时登录设备的 SSL VPN 用户的最大数值。

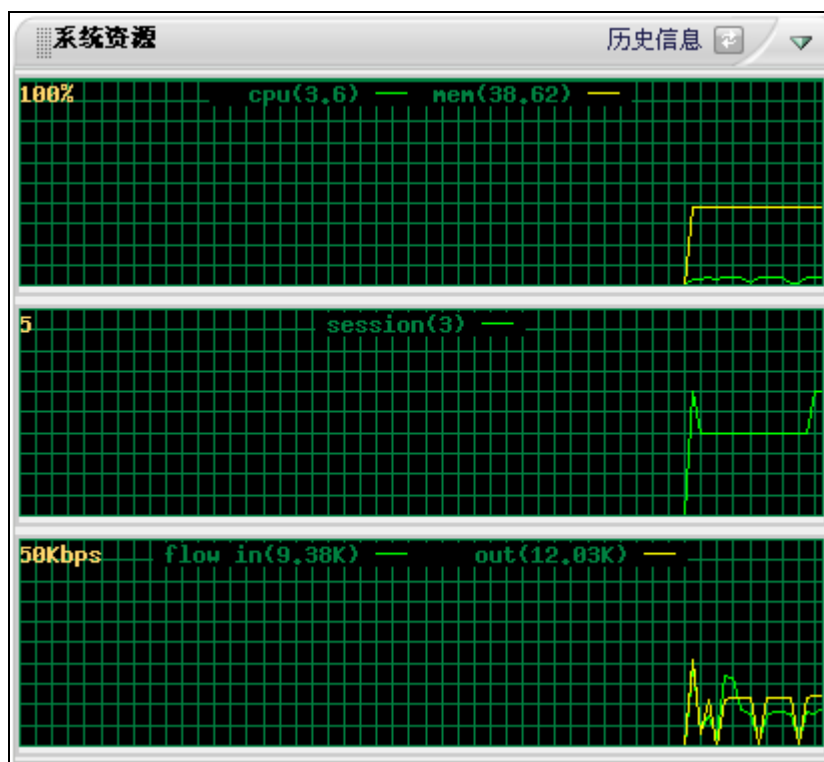
d) “警告信息”窗口显示系统日志中级别为“告警”、“严重”、“错误”和“警示”的日志信息。

根据警报信息可以跟踪设备的设置更改情况，每条信息中含有发布的时间与日期，以及报警内容。

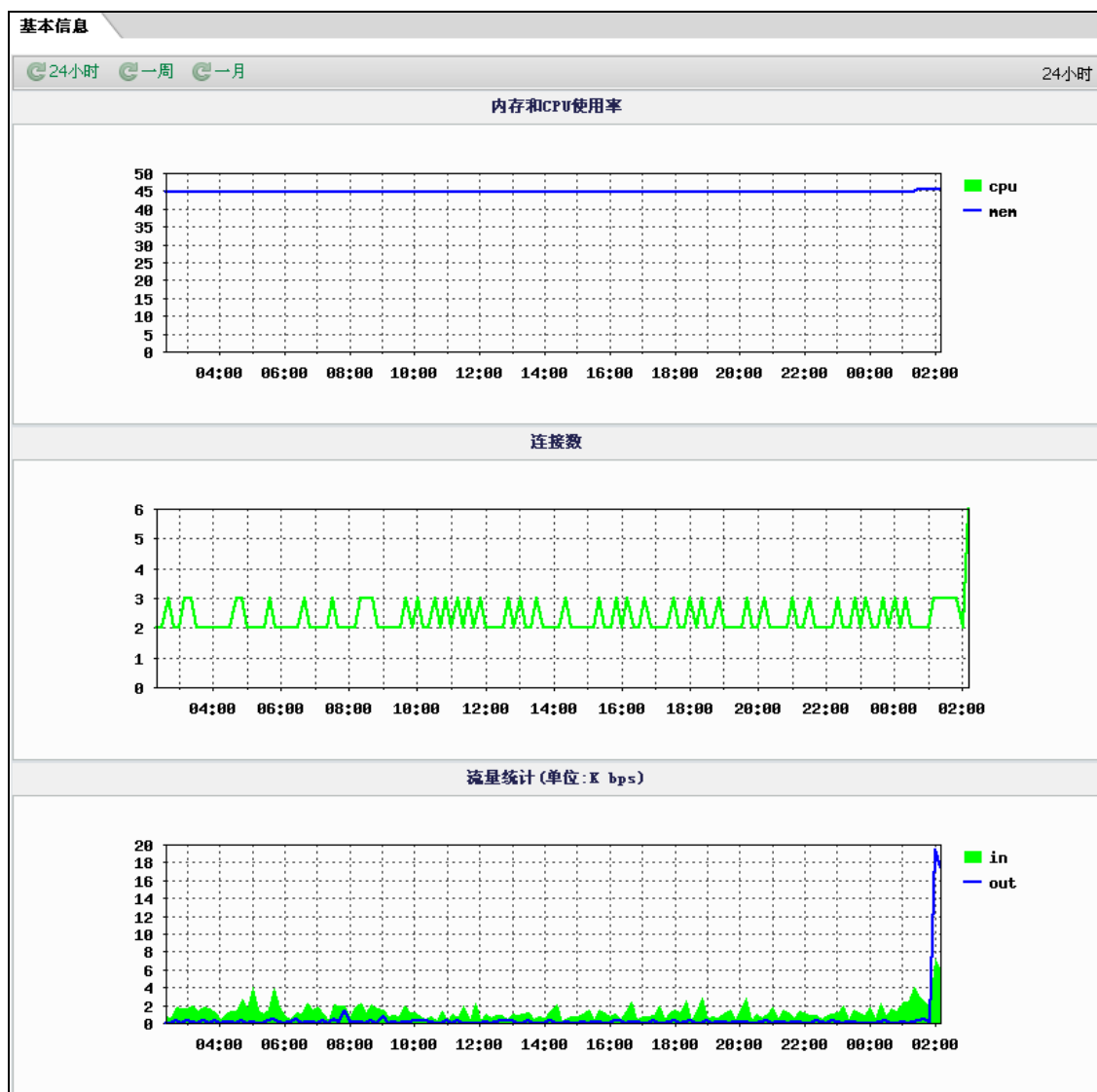


警告信息	
2010-06-23 01:47:17	type=system op="SERVER DO...
2010-06-23 01:47:04	type=system op="SERVER DO...
2010-06-23 01:46:51	type=system op="SERVER DO...
2010-06-23 01:46:38	type=system op="SERVER DO...
2010-06-23 01:46:25	type=system op="SERVER DO...
2010-06-23 01:46:15	type=system op="SERVER DO...
2010-06-23 01:46:02	type=system op="SERVER DO...

e) “系统资源”窗口显示设备的 CPU 和内存的占用百分比情况。



点击标题栏的“历史信息”按钮，系统如下图所示界面。



管理员可以点击相应的按钮，查看系统资源在二十四小时内、一周内或一月内的历史统计信息。

f) “病毒排行榜”窗口显示设备中防病毒模块发现最多的 10 个病毒。当设备不包含防病毒模块时不会显示该窗口。

g) “攻击排行榜”窗口显示设备中 IPS 模块实时检测到的攻击数排行列表。当设备不包含 IPS 模块时不会显示该窗口。

2) 最小化窗口

当界面中窗口较多时，可以点击窗口标题栏的图标将该窗口最小化。如下图，将“系统信息”窗口最小化。



最小化后界面如下图所示。



3) 移动窗口位置。

当管理员将鼠标置于窗口的标题栏时，按住鼠标左键不放，可以在界面中调整窗口的位置。

4) 刷新窗口显示内容。

管理员可以点击“”图标，刷新该窗口显示的最新信息。

4.2 配置

在 **系统管理 > 配置** 菜单中，管理员可以查看和修改系统设备名、管理员登录和管理系统的参数、对外开放系统服务、设置安全网关系统时钟、设置WEB管理，启动或停止对系统进行监控和管理的系统服务、设置TP服务器参数、设置SNMP协议参数等操作。

4.2.1 设置系统参数

用户可以设置管理员登录参数、连接超时参数以及查看会话的统计信息。系统参数规定同一管理员的最大登录失败次数，以及并发管理数和管理登录地点。一旦某个管理员的登录失败次数超过设定数值，系统将对其进行登录锁定，从而防止非法用户通过暴力破解的方式登录到网络卫士安全网关。

系统参数的设置步骤如下：

- 1) 选择 **系统管理 > 配置**，打开“系统参数”页签，如下图所示。



“基本属性”参数说明见下表：

参数	说明
设备名称	设定安全网关的系统名称，默认为 TopsecOS，在用户使用命令行时，初次使用或管理员未配置时，命令提示符显示为“TopsecOS#”。经过此处修改后，将显示为配置后的设备名称。

- 2) 点击“高级属性”可以修改系统其他参数。“网络参数”设置界面如下图：

网络参数		
已建立TCP连接超时	600	* [10-7200秒, 缺省600秒]
握手时TCP连接超时	20	* [10-200秒, 缺省20秒]
关闭时TCP超时时间	3	* [3-800秒, 缺省3秒]
UDP连接超时时间	60	* [10-7200秒, 缺省60秒]
其他类型连接超时	20	* [10-7200秒, 缺省20秒]
不超时最大百分比	20	* [5-90, 缺省20]
SYN代理参数	2000 配额	* [10-200000个/秒, 缺省2000个/秒]
	5000 限额	* [10-200000个/秒, 缺省5000个/秒]
连接类型配额	0 TCP	* [占总连接的百分比上限]
	0 UDP	* [占总连接的百分比上限]
	0 其他	* [占总连接的百分比上限]
ICMP重定向	关	
TCP reset	关	
包校验和	关	
连接完整性	开	
快速连接重用	关	
MPLS透传	关	
CDP透传	开	
智能选路	关	
扩展IP协议支持	[0-255, 多个协议值以空格分隔]	
应用		

参数说明如下表。

参数	说明
已建立 TCP 连接超时	设定 TCP 连接建立后的空闲超时，单位为秒。默认值为 600 秒。设定范围为 10-7200 秒。
握手时 TCP 连接超时	设定建立 TCP 连接时的超时时间，单位为秒。默认值为 20 秒。设定范围为 10-200 秒。
关闭时 TCP 超时时间	设定关闭 TCP 连接时的超时时间，单位为秒。默认值为 20 秒。设定范围为 3-800 秒。
UDP 连接超时时间	设定 UDP 连接建立后的空闲超时，单位为秒。默认值为 60 秒。设定范围为 10-7200 秒。
其他类型连接超时	设定其他连接建立后的空闲超时，单位为秒。默认值为 20 秒。设定范围为 10-7200 秒。
不超时最大百分比	指安全网关连接表中的长连接占设备的最大连接数的百分比，默认值为 20，设定范围为 5-90。 说明： 请注意不是指长连接占目前所有活动链接的百分比。例如，安全网关的最大连接数是 70 万，“不超时最大百分比”为 10，当设备上活动的长连接数达到 7 万的时候，安全网关会自动清空较早建立的 50%长连接，以释放系统资源。
SYN 代理参数	设定建立 SYN 代理时的每秒连接数目的限定。 配额，平均每秒 SYN 代理数目，默认为 2000 个/秒，设定范围

参数	说明
	为 10-200000 个/秒； 限额，最大每秒 SYN 代理数目，默认值为 5000 个/秒。设定范围为 10-200000 个/秒； 说明： SYN 代理限额应大于 SYN 代理配额。
连接类型配额	设定 TCP 连接、UDP 连接以及其他类型协议的连接信息占总连接的百分比上限值。默认为 0。输入范围为 0—99。其总和不能超过 100。
ICMP 重定向	设定是否允许设备发送 ICMP 重定向报文。
TCP reset	设定对违反安全策略的 TCP 连接，是否允许设备发送 TCP Reset 报文。
包校验和	对 TCP/UDP/ICMP/IP 的校验和进行检查。
连接完整性	对 TCP/ICMP 的连接状态进行检测，默认是打开的。
快速连接重用	当源到目的的连接已经存在，源向目的发送 SYN 包时，如果不设置该选项，则 SYN 包会被丢弃。只有打开该开关时才会将已建立的连接删除并重新建立连接。
MPLS 透传	只有当安全网关工作在透明模式时需要开启 MPLS 透传功能，路由模式时安全网关将直接丢弃 MPLS 报文。 透明模式下，如果开启 MPLS 透传功能，则可以对通过安全网关的 MPLS 报文进行安全策略控制；如果关闭 MPLS 透传功能，安全网关将直接转发 MPLS 报文。
CDP 透传	设置是否支持思科邻居发现报文穿越安全网关。
智能选路	设置是否开启智能选路功能。 可选值：开、关。 说明： 在多链路的环境中，通过设备转发或者到本机的报文会进行负载均衡。在实际环境中，会出现这样的情况：要求报文必须从其接收的端口原路返回，即不能让请求报文从一条链路来，而回复报文从另一条链路返回。此问题的解决方案是开启“智能选路”开关，就可以做到报文的源去源回。
扩展 IP 协议支持	网络卫士安全网关默认情况下只支持对协议 TCP、UDP、ICMP 和 GRE 建立连接，当用户需要支持更多的 IP 协议时，则需要在此设置。文本框中需要输入 IP 协议的协议类型值，可以一次输入多个，中间用逗号隔开即可。

3) 点击“应用”按钮，将系统参数的修改提交系统。

4.2.2 开放服务

为了保障设备的安全，在出厂配置中，如果不包含 SSL VPN 模块，则仅允许管理员通过 eth0 口使用 HTTPS 协议的 443 端口对设备进行 WEBUI 管理；如果包含 SSL VPN 模块，则仅允许管理员通过 eth0 口使用 HTTPS 协议的 8080 端口对设备进行 WEBUI 管理；禁止对设备其他端口的明文访问。

管理员通过开放服务，配置对本机端口的访问控制规则，允许设备在相应的物理接口接收用户的连接请求。请参见 4.2.2.2 开放服务。如果设备要接收管理员发出的管理或监控的连接请求，设备上相应的系统服务进程还必须处于“启动”状态，否则无法接收用户的连接请求。请参见 4.2.2.1 管理系统服务。

4.2.2.1 管理系统服务

系统服务指的是对设备进行管理或监控的服务，包括监控服务、SSH 服务、Telnet 服务和 NTP 服务。

- 监控服务：接收远程监控设备的请求。
- SSH 服务：接收 SSH 协议远程管理请求。
- Telnet 服务：接收 Telnet 协议远程管理请求。
- NTP 服务：网络卫士安全网关作为 NTP 服务器为其它网络设备提供 NTP 服务。

TOS 系统提供了对这些服务的控制（启动和停止）功能，其具体的操作如下：

- 1) 选择 **系统管理 > 配置**，选择“开放服务”页签，如下图所示。



- 2) 点击相应服务的“启动”或“停止”按钮即可完成该服务的启动或停止操作。

4.2.2.2 开放服务

管理员通过开放服务来设置对设备的本机端口进行访问控制的规则。系统可管理的服务分为以下几类：

服务名	意义
GUI	允许用户通过网络卫士安全网关管理器对设备进行配置和管理。
WEBUI	当安全网关不包含 SSL VPN 模块时，开放该服务用于允许用户通过 WEBUI 的 443 端口对设备进行配置和管理。 当安全网关包含 SSL VPN 模块时，要实现管理员通过 WEBUI 对设备进行管理无需开放该服务，只需开放 SSLVPNMGPR 服务。要实现普通用户通过 443 端口访问设备时只需开放 SSLVPN 服务。
AUTH	允许用户使用安全网关设备所提供的认证机制。
CGI_AUTH	允许 CGI 认证用户使用安全网关设备所提供的认证机制。
UPDATE	允许用户通过 TOPSEC 管理中心对设备进行远程升级。

服务名	意义
MONITOR	允许用户根据其设定的条件监控设备的运行状态。
SNMP	允许设备与 SNMP 管理主机进行通信。
PING	允许用户可以 PING 到设备的物理接口地址、VLAN 虚接口和子接口的地址。
SSH	允许用户通过 SSH 方式对设备进行配置和管理。
TELNET	允许用户通过 TELNET 对设备进行配置和管理。
TOSIDS	允许与 IDS 设备间的联动。
DHCP	允许设备作为 DHCP 服务器、DHCP 客户端或 DHCP 中继使用。
IPSecVPN	允许设备与 VPN 设备建立 IPSec VPN 隧道进行通信。
RIP	允许使用 RIP 动态路由协议。
L2TP	允许 L2TP 客户端登录。
PPTP	允许 PPTP 客户端登录。
NTP	允许系统使用 NTP 协议保持设备本身和其他设备的时钟同步。
SSLVPN	当安全网关包含 SSL VPN 模块时，才包含该选项，用于开放 443 和 4430 端口，允许使用 SSLVPN 的相关功能，包括全网接入、普通用户登录网关等。
SSLVPNMGR	当安全网关包含 SSL VPN 模块时，才包含该选项，用于管理员通过 8080 端口对安全网关进行管理。
WEBSV	当防火墙包含 SSL VPN 模块时，才包含该项，用于开放 SSL VPN 用户使用 WEBUI 方式进行认证和端口转发的功能。
BGP	允许使用 BGP 动态路由协议。

开放服务的具体设置方法如下：

1) 选择 **系统管理 > 配置**，选择“开放服务”页签，右侧页面显示已有的服务控制规则，如下图所示。



红色框内为出厂配置中已经开放的服务，请参见 [3.1.8本机服务访问控制规则](#)。

2) 添加规则

a) 点击“添加”，进入添加服务页面，如下图所示。

The screenshot shows a dialog box titled "添加配置" (Add Configuration). It has three dropdown menus for configuration: "服务名称" (Service Name) set to "GUI", "控制区域" (Control Area) set to "area_eth0", and "控制地址" (Control Address) set to "webserver [主机]". Below these are two buttons: "确定" (Confirm) and "取消" (Cancel).

b) 参数说明如下表。

参数	说明
服务名称	选择需要开放的服务。
控制区域	准许来自哪些区域的访问使用该服务。
控制地址	准许来自哪些地址对象（包括主机、范围和子网类地址对象）的访问使用该服务。地址对象设置请参见 7.1 设置地址资源 。

c) 点击“确定”，则该服务规则将被添加到列表中。

3) 修改规则

点击对应的“修改”图标可以修改已设定的规则。

4) 删除规则

点击对应的“删除”图标，可以删除该规则。

4.2.3 设置系统时间

安全网关系统的内置时钟，是安全网关系统记录日志信息、访问控制、QoS 控制、报警等事件的时间基准，因此安全网关的时间的精确性会对这些事件产生直接影响。安全网关为了解决此类问题提供了系统时间管理功能，用户可以简单地手工修改安全网关时钟；也可以作为 NTP（Network Time Protocol）客户端，根据设定的 NTP 服务器上的时间来同步安全网关的系统时钟。

说明

- ✧ 用 NTP 服务器更新系统时钟时，请确认远程的 NTP 服务器工作正常，并启动了该项服务。
- ✧ 修改安全网关系统时间后，用户必须重新登录。

系统时钟设置方法为：

1) 选择 **系统管理 > 配置**，选择“时间”页签，可以进行时钟的相关设置，如下图所示。

2) 在“系统时间”区域，用户可以查看和设置安全网关设备当前的时区、日期和时间。

值得注意的是，页面上显示的时区、日期和时间都是最后一次打开该页面时获取的系统数据，不会实时更新，如要查看当前的时间数据，请点击页面右上角的“刷新页面”，或点击“刷新”按钮。

3) 修改系统时间

管理员可以在“手动设置”处，手工修改时区、日期和时间的设置，点击“应用”按钮完成修改。操作成功，系统会要求用户重新登录。

4) 使用 NTP 服务器同步系统时钟

网络卫士安全网关可以使用 NTP 协议，使系统时间与指定时间服务器的时间同步。

在“与 NTP 服务器同步”处设置 NTP 服务器的 IP 地址，安全网关支持两种时间更新方式：定时更新和立即更新。

a) 定时更新方式：点击“应用”按钮，设备会作为 NTP 客户端，自动和 NTP 服务器保持时间的同步。

b) 立即更新方式：点击“立即同步”按钮，实现和指定的 NTP 服务器时间的立即同步。

4.2.4 SNMP

网络卫士安全网关支持 SNMP（Simple Network Management Protocol，简单网络管理协议）管理，网络卫士安全网关可以响应 SNMP 管理主机的查询，向 SNMP 管理主机返回相应的运行状态信息，包括各个接口流量统计、差错率、带宽占用率等属性，IDS 攻击统计情况，以及查询 VPN 隧道信息。网络卫士安全网关支持主流的 SNMP 管理软件，如 HP 的 Open View 等等。

同时也可以根据系统内部设定，主动地向SNMP管理端发送TRAP消息。网络卫士安全网关已经预定义了TRAP事件，具体请参见 [17.3.2设置触发报警的安全事件](#)。用户无须设定TRAP事件，在一定程度上也减少了误操作的可能性并提升了系统的安全性。

如果要通过 SNMP 管理网络卫士安全网关，用户需要进行如下设置：

1) 首先，需要在管理主机和陷阱主机上安装SNMP管理软件（比如HP OPENVIEW 软件）、在管理主机上导入公有MIB库或TOPSEC MIB库（可从随机光盘中获得）并做简单配置，SNMP管理端的配置具体操作请参见附录 B简单网络管理协议SNMP。

2) 启动SNMP服务，否则无法利用SNMP协议管理安全网关，也无法支持SNMP报警。具体操作请参见 [4.2.4.1 SNMP代理服务控制](#)。

3) 对SNMP管理区域的管理主机开放SNMP服务。具体操作请参见 [4.2.2.2开放服务](#)。

4) 设置管理主机对象。具体操作请参见 [4.2.4.2管理主机](#)。

5) 设置陷阱主机对象以接收TRAP消息。具体操作请参见 [4.2.4.3陷阱主机](#)。

6) 如果是采用SNMPV3 版本，则需要添加SNMP V3 用户。具体操作请参见 [4.2.4.4 SNMPV3 用户](#)。

7) 使SNMP设置生效。具体操作请参见 [4.2.4.1 SNMP代理服务控制](#)。

4.2.4.1 SNMP 代理服务控制

安全网关上必须启动 SNMP 代理服务才能对安全网关进行 SNMP 管理以及进行 SNMP 报警。修改参数的配置后，管理员必须重新启动 SNMP 服务才能使参数生效。

设置方法为：

1) 选择 **系统管理 > 配置 > SNMP**，在“SNMP服务控制”处设置，如下图所示。

SNMP服务控制	位置	www.topsec.com.cn
	联系	support@topsec.com.cn
应用 启动 停止		

2) 设置参数

“位置”用于标识设备本身在网络环境中的位置，此项为可选输入项，默认显示为“www.topsec.com”；

“联系”用于输入设备的直接责任人的联系方式，可以为电话号码或 Email 地址，通过配置此参数，将重要信息存储在安全网关中，以便出现紧急问题时查询使用。此项为可选输入项，默认显示天融信公司客服的邮件地址。

3) 点击“应用”按钮保存参数修改。如果没有修改默认参数，可以略去此步骤。

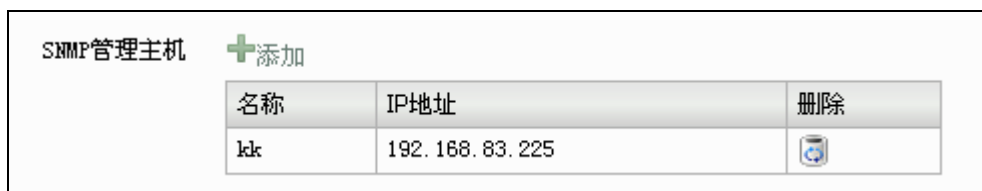
4) 点击“启动”按钮，安全网关上的 SNMP 代理服务将被启动。也可以点击“停止”按钮停止 SNMP 代理服务。

4.2.4.2 管理主机

管理主机安装 SNMP 管理软件并导入了公有 MIB 库或 TOPSEC MIB 库后，还需要在安全网关上添加管理主机信息，对于 V3 用户还需要设置认证密码和私钥，才能够查询安全网关设备信息。

设置方法为：

选择 **系统管理 > 配置 > SNMP**，在“SNMP管理主机”处进行设置，如下图所示。



界面显示已经添加的管理主机对象。点击“添加”进入如下图的界面。

参数说明如下图所示。

参数	说明
主机名称	添加该管理主机的名称。
管理主机类型	设置管理主机的类型，可选值为“主机”和“子网”。 “主机”指设定 SNMP Manager 为一台主机；“子网”指设定 SNMP Manager 为一个子网，该子网内的主机都可以配置为 SNMP 管理主机。

参数	说明
	说明： 1. 当管理主机只有一个时，添加“主机”类型的管理主机对象。 2. 当管理主机具有多个且正好位于一个子网时，可以添加多个“主机”类型的管理主机对象，也可以添加一个“子网”类型的管理主机对象。
主机 IP	当管理主机类型为“主机”时，用于指定 SNMP 管理主机对象的 IP 地址。 当管理主机类型为“子网”时，用于指定 SNMP 管理子网对象的子网地址及其掩码。
Community	指定 SNMP 管理主机访问安全网关时的团体名。

设置参数完成后，点击“确定”完成管理主机对象添加。新添加的管理主机对象会显示在管理主机列表中。

3) 删除管理主机对象。选择某管理主机对象，点击对应的“删除”图标可以删除该管理主机。

4.2.4.3 陷阱主机

陷阱主机是指接收安全网关发出 SNMP Trap 消息的主机。

设置方法为：

1) 选择 **系统管理 > 配置 > SNMP**，在“SNMP陷阱主机”处设置，如下图所示。

SNMP陷阱主机 		
名称	IP地址	删除
snmpghost	192.168.96.71	

界面显示已经添加的陷阱主机对象。

2) 添加陷阱主机对象。点击“添加”进入如下图的界面。

SNMP陷阱主机	
主机名称	*
主机IP	*
确定 取消	

上图中，在“主机名称”处输入要增加的陷阱主机对象的名称。在“主机 IP”处指定陷阱主机的 IP 地址。

点击“确定”完成陷阱主机对象的设置，新添加的对象会显示在陷阱主机列表中。

3) 删除陷阱主机对象。选择某陷阱主机对象，点击对应的“删除”图标可以删除该陷阱主机对象。

4.2.4.4 SNMPV3 用户

网络卫士安全网关 3.3 版本支持 SNMP V3 版本，同时兼容 V1 和 V2 版本。当用户使用 SNMP V1、SNMP V2 对安全网关进行网络查询时，只需在管理主机设置时设置

“community”即可，但存在的最大问题是传输的认证和管理数据没有加密、数据的收发缺乏鉴别机制，因此对网络的管理缺乏安全保障。当使用 SNMP V3 对安全网关设备进行查询时，不仅将传送的信息使用 DES 算法进行加密，而且还需设置 SNMPV3 用户的密钥，以便安全网关验证用户身份，因此进一步提高了对安全网关设备进行 SNMP 管理的安全性。

具体设置方法为：

- 1) 选择 **系统管理 > 配置 > SNMP**，在“SNMPV3 用户”处设置，如下图所示。

- 2) 点击“添加”可以添加 SNMPV3 用户，界面如下图所示。

参数说明如下表所示。

参数	说明
用户名称	添加该用户的名称。
安全级别	设置是否对 SNMP 认证和管理信息进行加密。可选项为：加密、不加密。当设置加密时，同时使用加密和认证技术，先对数据进行加密，然后进行认证技术的消息摘要计算。设置不加密时，只使用认证技术。
认证密码	指定 SNMPV3 用户对象进行认证时使用的密码，加密方式为 MD5。必须为 8 位字符。
私有密码	指定消息加密时使用的密码，加密方式为 DES。必须为 8 位字符。

点击“确定”，完成用户添加，新添加的用户将显示在 SNMPV3 用户列表中。

- 3) 修改已有用户属性。选择某用户，点击对应的修改图标可以修改该用户的属性。
- 4) 删除用户。选择某用户，点击对应的删除图标可以删除该 SNMP V3 用户。

4.2.5 邮件设置

当网络卫士安全网关截获违反规则的邮件时，系统会向收件人发送警告邮件。此时需要管理员设置发件人的地址信息、邮件帐户名和密码信息，以及该帐户的 SMTP 服务器地址。设置步骤为：

- 1) 选择 **系统管理 > 配置**，并激活“邮件设置”页签，界面如下图。

参数说明如下表所示：

参数	说明
邮件服务器地址	设置转发邮件的发件人帐户的 SMTP 服务器地址或域名，地址需符合 IP 地址格式。 说明： 如果服务器配置地址为域名，管理员一定要在 网络管理 > 域名解析 处配置安全网关的 DNS 服务器，否则不可能生效。
服务器端口	设置转发邮件时的 SMTP 服务器端口号。
身份验证	设置邮件服务器是否需要发件人的身份进行认证。
帐户名	当勾选“认证”后，需要设置该参数。设置发送转发邮件的帐户名。
密码	当勾选“认证”后，需要设置该参数。设置发送转发邮件的帐号密码。
发件人地址	当勾选“认证”后，需要设置该参数。设置接收违反规则的转发原邮件的发件人地址，需符合邮件地址格式。

点击“清空配置”，将删除界面中所有设置的参数。

- 2) 点击“应用”，使参数设置生效。

4.2.6 短信设置

为了提高VRC客户端认证的安全性，对VRC用户增加手机认证功能。VRC客户端认证成功后，如果其所属角色开启“强制短信认证”开关（请参见 8.2.1角色管理），网关会产生动态口令，并且根据本节设置的参数向用户发送动态口令。本节介绍短信认证服务器的相关参数设置。具体步骤为：

- 1) 选择 **系统管理 > 配置**，点击“短信设置”页签，界面如下图所示。

- 2) 设置短信中转服务器。

在“短信设置”处设置相关参数，参数说明如下表所示：

参数	说明
发送短信方式	根据短信网关是否直接连接安全网关，设置发送短信的模式。可选项为： 短信服务器和本地。 说明： 当设备所在的机房屏蔽无线电信号时，需要通过网络先将短信发送到短信中转发送服务器，再发送短信。此时需要选择“topsec 短信服务器”；否则，选择“本地”即可，表示短信网关直接连接在安全网关的 USB 口。
服务器地址	设置短信中转发送服务器的 IP 地址。 只有当“发送短信方式”选择“短信服务器”时才需要设置该项。
端口	设置短信中转发送服务器接收网络卫士安全网关设备发送的短信的端口。 只有当“发送短信方式”选择“短信服务器”时才需要设置该项。
共享密钥	设置由短信中转服务器指定的认证共享通行串，必须与短信中转发送服务器的设置一致。

参数	说明
	只有当“发送短信方式”选择“短信服务器”时才需要设置该项。
网关 ID	设置由短信中转服务器指定的用于标识网络卫士安全网关的 ID 号。只有当“发送短信方式”选择“短信服务器”时才需要设置该项。
认证超时时间	设置认证超时值。当发送短信时间达到此处设定的值后，密钥需要重新协商。只有当“发送短信方式”选择“短信服务器”时才需要设置该项。

点击“应用”完成参数设置。点击“清空配置”，则删除当前所有设置的参数信息。

3) 短信发送测试

设置接收信息的手机号码，然后点击“测试”按钮，可以测试安全网关是否能正确地向设置的手机发送动态口令。

4.2.7 WEB 管理

在本节点设置对安全网关通过 WEBUI 界面进行管理的相关参数设置。

具体操作如下：

1) 选择 **系统管理 > 配置**，并点击“WEB管理”页签，如下图所示。



2) 开启管理员证书认证功能

在“认证方式”处设置是否开启“验证客户端证书”功能，默认不启动，管理员只需通过用户名/密码认证即可登录安全网关。

勾选“开启”，并点击“设置”按钮，则当前管理员退出 WEBUI 界面。管理员再次登录系统时，需要同时通过证书认证和用户名/密码认证，才能登录网络卫士安全网关。

相关的配置有：

a) 向管理员签发证书

可以使用设备本地CA向管理员签发证书，具体请参见 [12.3.2 签发证书](#)；也可以使用第三方CA向管理员签发证书，此时在安全网关上需要设置第三方CA的根证书及其CRL列表，具体请参见 [12.2 第三方CA证书](#)。

b) 管理员导入证书

在管理员所在主机上将 PKCS#12 格式的个人证书导入到 Internet 浏览器中。

3) 设置安全网关作为 SSL 服务器的证书

管理员通过 SSL 协议对安全网关进行管理，服务器证书用于让管理员利用浏览器验证安全网关设备的真实身份，并且通过服务器证书和私钥进行具有 SSL 加密的通信过程。出厂配置中内置了安全网关证书，管理员可以在“服务器证书”处导入新的设备证书和私钥，新导入的证书将覆盖已有的证书。

a) 点击“导入”，弹出证书导入界面，如下图。



该对话框标题为“服务器证书、私钥的导入”。它包含三个单选按钮，分别对应不同的证书格式：PEM证书（当前被选中）、DER证书和PKCS#12证书。对于每种格式，都有相应的输入框和“浏览...”按钮。PEM格式需要输入证书和私钥；DER格式也需要输入证书和私钥；PKCS#12格式需要输入证书和证书密码。对话框底部有两个按钮：“确定”和“取消”。

格式	证书	私钥	其他
☒ PEM证书	浏览...	浏览...	
☐ DER证书	浏览...	浏览...	
☐ PKCS#12证书	浏览...		证书密码

b) 首先选择导入证书的格式，可选项为“PEM 证书”、“DER 证书”和“PKCS#12 证书”。

c) 点击“浏览”按钮导入服务器的证书和私钥，即由 CA 为安全网关设备签发的证书和私钥。

关于证书的使用和获取，请咨询企业内部的证书管理员。如果新导入的证书名称和安全网关登录接口的 IP 地址同名，下次登录时将不再弹出安全提示窗口。

d) 点击“确定”完成证书导入。

4.2.8 TP 注册

TopPolicy（以下简称 TP）是由天融信公司开发的安全设备与策略管理系统，用于对网络中的安全设备进行集中管理与监控，负责为设备发放证书、管理各设备之间建立隧道的策略、控制设备的注册，以及收集设备登录时的 IP 地址、子网掩码、IP 是否经过了 NAT 等重要信息。要实现 TopPolicy 对安全网关的管理，需要在安全网关上设置 TP 服务器的信息，设置完成后网络卫士安全网关将自动向 TP 服务器进行注册并下载相关策略，把安全网关的相关信息发送到 TP 服务器。

网络卫士安全网关支持主、从 TP 服务器的工作方式，设备首先向主 TP 服务器进行身份认证并下载策略，当主 TP 服务器不能正常工作时，设备将尝试向从 TP 服务器进行身份认证并下载策略。用户在采用证书认证建立隧道时需要对主服务器设置，并且根据实际情况选择设置从服务器。

设置 TP 服务器的具体操作如下：

1) 点击导航菜单 **系统管理 > 配置**，并选择“TP注册”页签，界面如下图所示。

系统参数	开放服务	时间	SNMP	邮件设置	短信设置	WEB管理	TP注册
服务器类型	地址或域名	认证状态	TP服务器位置	修改			
主服务器	0.0.0.0	未认证	外部				
从服务器	0.0.0.0	未认证	外部				

2) 点击对应的修改图标，进行主/从 TP 服务器的设置，如下图。

TP注册设置

设置选择

服务器地址

服务器域名

通告端口

策略端口

TP服务器位置

IP地址 ▼

外部 ▼

确定
取消

3) 设置页面中的各参数，参数说明如下表。

参数	说明
设置选择	有两个值，“IP 地址”和“域名”。 选择“IP 地址”则需在下面的服务器地址处输入 TP 服务器的 IP 地址； 选择“域名”则需在服务器域名处输入 TP 服务器的域名。
服务器地址	TP 服务器 IP 地址。当“设置选择”处选择“IP 地址”时需要设置该参数。
服务器域名	TP 服务器域名。当“设置选择”处选择“域名”时需要设置该参数。
通告端口	设备向 TP 服务器发送 UDP 通告包的端口，设备向 TP 服务器发送周期性的保活通告、以及 TP 发送给设备的一些反向通告都使用这个端口，默认端口为 2010，范围 0-65535。
策略端口	设备使用 TCP 协议从 TP 服务器下载 VPN 策略的端口。默认端口为 2010，范围 0-65535。 说明： 1) 只有当设备包含 IPSec VPN 模块，而且采用 TP 集中管理模式时，才需要设置该参数。 2) TP 通过 TCP 协议的 4000 端口向设备下发安全网关模块相关的策略以及 IPS 策略，因此下发只需要开放 GUI 服务，和此参数无关。

参数	说明
TP 服务器位置	当设备包含 IPSec VPN 模块，而且采用 TP 集中管理模式时，才需要设置该参数。 如果设备通过 IPSec 虚接口绑定的物理接口就可以向 TP 服务器发送通告包，则设置为“外部”； 当网关和 TP 之间的通告包通过 ipsec 虚接口绑定的物理接口发出去后，无法到达 TP 时，要把 TP 服务器的位置设置为“内部”，这时候网关和 TP 之间的通告包会通过系统的路由表，自动选择从哪个物理接口发出去。

4) 点击“确定”按钮，完成 TP 服务器的设置。

4.3 维护

在 **系统管理 > 维护** 菜单中，管理员可以对安全网关系统将进行维护工作，包括对系统的配置文件进行查看、上传、下载等操作，下载设备的健康记录，对设备进行升级，设备恢复出厂默认配置、重新启动设备等功能。

4.3.1 配置维护

系统配置指的是整个安全网关中各个功能模块的配置和文件，包括安全网关配置（包括网络基本配置）、VPN 配置、AV 配置。

系统配置基本上可以分为三种：

- 运行配置，指的是设备当前运行状态下的配置情况，该配置可以随用户的操作而动态调整，当系统重新启动后，该配置失效。
- 存盘配置，指的是用户最后一次手工保存在设备上的配置文件，当系统重新启动后，会自动加载该配置文件。
- 备份配置，指的是用于备份的存盘配置，通常是某一历史时刻的存盘配置。备份配置只存在于 V3.3.006 之后的 TOS 版本。

另外，系统还提供了对设备配置进行维护的功能，用户可以方便地进行上传/下载配置文件、导出部分配置等维护操作。

维护配置的操作方法如下：

- 1) 选择 **系统管理 > 维护**，选择“配置维护”页签，出现如下页面。

配置维护		系统升级	重启	健康记录	诊断	服务更新
配置维护						
配置替换			浏览...			
	替换运行配置					
配置下载	☐ 加密 ☒ 运行配置 ☐ 存盘配置 ☐ 备份配置					
	下载					
存盘配置备份						
复制主配置到备份配置	复制		备份配置最近保存时间	N/A.		
复制备份配置到主配置	复制		主配置最近保存时间	+00 2010-06-18 07:20:14		
批量配置处理						
部分导出	☐ 地址 ☐ 服务 ☐ 时间 ☐ 阻断策略 ☐ 安全策略 ☐ 用户角色					
	下载					
部分导入	☒ 选择文件 浏览...					
	☐ 输入配置					
	上传					
实时操作	实时操作					

2) 配置维护。配置维护是指对安全网关上的配置文件进行下载备份或上传更新。

配置维护	
配置替换	浏览...
	替换运行配置
配置下载	☐ 加密 ☒ 运行配置 ☐ 存盘配置 ☐ 备份配置
	下载

a) 配置替换

配置替换是指把本地管理主机上备份的配置文件上传到设备，作为设备的保存配置，同时自动加载到运行配置。替换配置文件后，需要管理员重新登录网络卫士安全网关。

点击“浏览”，选择配置文件所在的目录。然后点击“替换运行配置”，则将本地保存的配置文件加载到设备上，则新加载的配置文件替换设备原来的配置文件。

b) 配置下载

配置下载是指导出系统的运行配置、存盘配置或备份配置文件，并将其保存在管理主机指定目录中。

首先，需要选择下载的配置文件类型：“运行配置”、“存盘配置”或“备份配置”。

其次，选择是否以加密形式下载配置文件，勾选“加密”后，下载的配置文件为“密文”方式；否则为“明文”方式。

然后，点击“下载”按钮，按钮下方增加蓝色提示性文字，如下图所示。

配置下载

加密 ☐ ☒ 运行配置 ☐ 存盘配置 ☐ 备份配置

下载

当前运行配置点击下载[明文][或用右键另存]

点击此链接或点击鼠标右键菜单中选择“目标另存为”，可以将系统当前运行的配置文件保存到管理主机本地的文件夹中。

3) 备份配置

此功能仅适用于 3.3.006 之后的版本。

当软件版本小于 3.3.006 版本时，只有当前配置，不存在备份配置。升级至 3.3.006 时，系统会自动将升级之前存储的配置文件作为备份配置文件保存在设备中。

管理员可以点击“复制主配置到备份配置”右侧的“复制”按钮，利用当前配置文件更新备份配置文件；

也可以点击“复制备份配置到主配置”右侧的“复制”按钮，在系统出现故障时使用备份配置文件替换当前的配置文件。

存盘配置备份			
复制主配置到备份配置	复制	备份配置最近保存时间	N/A.
复制备份配置到主配置	复制	主配置最近保存时间	+00 2010-06-18 07:20:14

4) 配置导入导出

a) 配置导出

是指将安全网关上已定义的访问控制策略、阻断策略和地址、服务、时间等资源进行下载到管理器主机进行备份。

勾选“地址”、“服务”、“时间”、“阻断策略”、“安全策略”或“用户角色”后的选择框，并点击“下载”按钮，界面上出现下载链接，如下图。

批量配置处理

部分导出

地址 ☒ 服务 ☒ 时间 ☒ 阻断策略 ☒ 安全策略 ☐ 用户角色 ☐

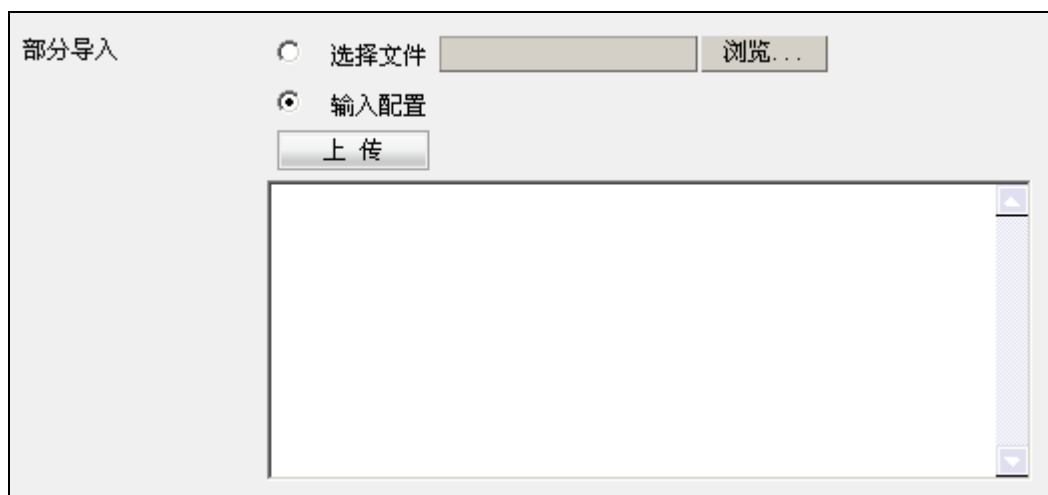
下载

点击下载[或用右键另存]

点击链接进行配置文件下载操作。

b) 配置导入

指的是将已经下载的配置文件重新导入设备，或者批量导入多条配置命令。



参数说明如下表所示：

参数	说明
选择文件	是指利用上传的配置文件更新当前安全网关上的策略或资源配置。点击“浏览”按钮选择要上传的配置文件，并点击“上传”按钮，系统将对上传的配置文件作合法性检查，不允许上传超过 3M 的配置文件，配置文件格式不合法也会作出提示。
输入配置	通过在文本框中一次输入多个命令，然后点击“上传”按钮，可以一次将多个配置命令批量上传到安全网关。 说明： 命令输入格式请参见《TopGate 命令行手册——基础配置》。

c) 实时操作，是指实时输入系统命令，一次只能输入一条命令。

点击“实时操作”按钮后，弹出如下图的窗口。



在文本框内输入完整的命令后，回车即可查看命令执行结果。如下图所示。



点击“清屏”，则删除文本框中所有信息。

4.3.2 系统升级

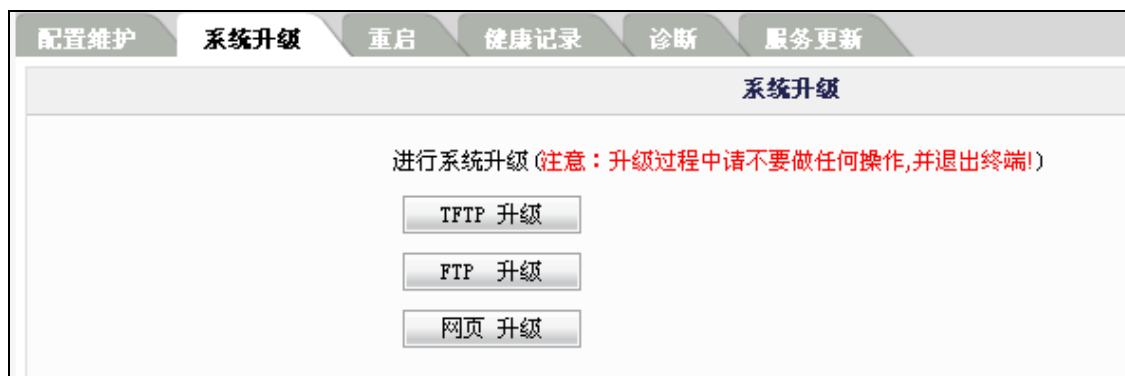
设备支持基于 TFTP 服务器、FTP 服务器和 WEBUI 系统的升级方式，以使用户方便、及时地使用天融信不断发布的升级包对设备的性能和功能进行扩充。系统升级前将会首先检查升级包与设备的硬件平台是否一致，如果不一致，系统会提示管理员不能进行升级操作。

说明

- ✧ 远程升级时，建议利用 FTP 或 TFTP 服务器进行升级，最好不要选择 WebUI 方式升级。
- ✧ 建议用户在升级前先保存系统的配置文件，如果升级后旧版本的配置文件与新系统不兼容，可通过随机光盘中的 ConfigTransfer.exe（路径：Tools/ConfigTransfer.exe）工具进行配置文件的格式转换。
- ✧ 系统支持从任意版本升级至 3.3 版本。

系统升级步骤为：

- 1) 选择 **系统管理** > **维护**，选择“系统升级”页签，进入系统升级界面。



2) 升级系统

➤ 通过 TFTP 服务器升级

在升级之前需要事先配置好 TFTP 服务器及其工作目录，并保证升级文件存放在工作目录中。

a) 点击“TFTP 升级”按钮，弹出如下图的系统升级对话框。



The image shows a dialog box titled "TFTP 升级". It contains two input fields: "服务器地址" (Server Address) and "文件名称" (File Name), both marked with a red asterisk indicating they are required. Below these fields is a button labeled "升级系统" (Upgrade System). At the bottom of the dialog is a long, empty text box.

在“服务器地址”处输入 TFTP 服务器的 IP 地址，在“文件名称”处输入升级包文件的完整名称。

b) 点击“升级系统”按钮，开始升级。

➤ 通过 FTP 服务器升级

在升级之前需要事先配置好 FTP 服务器及其工作目录，并保证升级文件存放在工作目录中。

a) 点击“FTP 升级”按钮，弹出如下图的系统升级对话框。



The image shows a dialog box titled "FTP 升级". It contains four input fields: "服务器地址" (Server Address), "文件名称" (File Name), "用户名" (Username), and "密码" (Password), all marked with a red asterisk indicating they are required. Below these fields is a button labeled "升级系统" (Upgrade System). At the bottom of the dialog is a long, empty text box.

参数说明如下表。

参数	说明
服务器地址	输入 FTP 服务器的 IP 地址。
文件名称	输入升级包文件的完整名称。
用户名/密码	分别输入登录 FTP 服务器的用户名称和密码。

参数	说明
	说明： 网络卫士安全网关通过 FTP 服务器升级时，支持匿名方式进行升级，因此用户名/密码也可为空。

b) 点击“升级系统”按钮，开始升级。

➤ 通过 WEBUI 网页升级

通过 WebUI 网页进行升级时，请尽量退出串口登录。

a) 点击“网页升级”按钮，弹出如下图的系统升级对话框。



b) 点击“浏览”按钮选择升级包。

c) 点击“升级系统”按钮，开始升级。

3) 升级成功后，系统自动重新启动，管理员与网络卫士安全网关的连接断开，需要等待片刻之后才能重新登录成功。

需要注意的是，如果系统长时间显示“正在升级，请稍等”对话框，则表明升级不成功，请重点考虑和检查以下几方面的原因：

- (1) 是否正确配置了升级服务器；
- (2) 是否输入了正确的文件名称或选择了正确的升级包。

4.3.3 重启

网络卫士安全网关管理员可以重启系统，具体的操作为选择 **系统管理 > 维护**，选择“重启”页签，如下图。



点击“重新启动系统”按钮，设备将会重新启动，系统通信暂时中断。

4.3.4 健康记录

管理员可以下载设备的健康记录，以便当设备出现异常时，可以帮助天融信的技术支持人员快速地定位并解决故障。

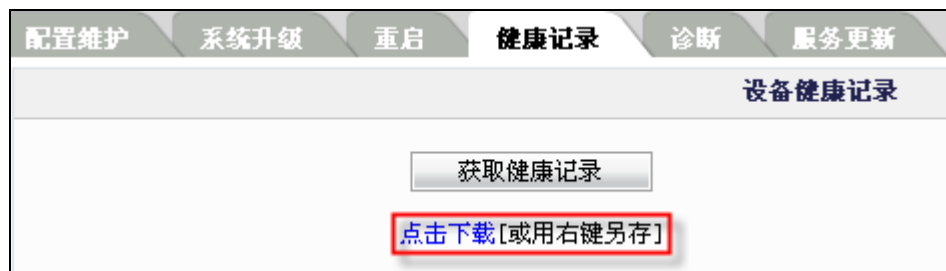
说明

◇ 健康记录仅供厂家调试人员使用，已加密。

1) 选择 **系统管理 > 维护**，选择“健康记录”页签，进入健康记录导出界面，如下图所示。



2) 点击“获取健康记录”按钮，系统自动生成当前的健康记录，并提示下载链接，如下图所示。



3) 根据提示，直接点击该链接或使用右键另存，保存健康记录到管理主机。

4.3.5 诊断

网络卫士安全网关提供 Ping 工具，用于探测网络连接状况，提供 TraceRoute 工具用于显示路由封包到达目的地址的信息。

诊断工具使用方法为：

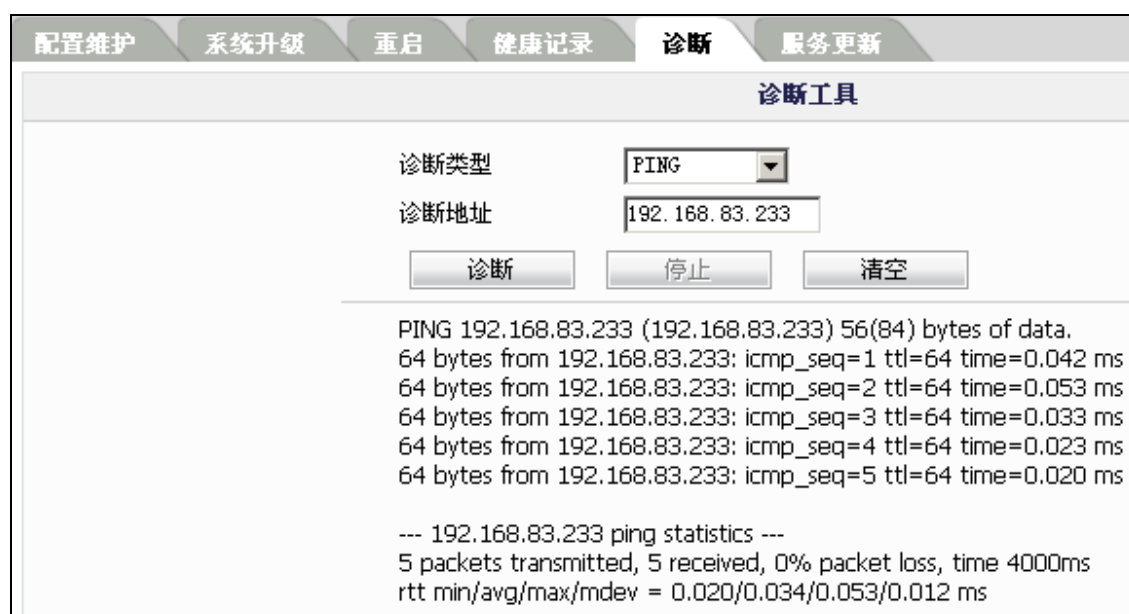
1) 点击导航菜单 **系统管理 > 维护**，并选择“诊断”页签，界面如下图所示。



2) 在“诊断类型”处选择使用的工具，可选项为“Ping”工具和“TraceRoute”工具。

在“诊断地址”处，输入探测的 IP 地址。

点击“诊断”按钮，在下方将显示命令的执行结果，如下图所示。



在探测过程中，点击“停止”按钮可以停止命令执行。如果探测停止，“停止”按钮自动显示为灰色不可操作状态。

点击“清空”按钮可以将命令的执行结果从 WEBUI 界面中删除。

4.3.6 服务更新

本节介绍病毒库及其许可证、入侵防御规则库、应用识别规则库以及 URL 库的更新方式。

4.3.6.1 更新病毒库及许可证

网络卫士安全网关基于病毒库进行病毒防御，病毒库的有效期限则是由许可证来控制的。

系统提供病毒库的在线升级和离线升级功能，确保设备上的病毒库保持最新的状态。还提供许可证文件更新功能来延长病毒库的有效期限。

具体设置步骤为：

1) 点击导航菜单 **系统管理** > **维护**，并选择“服务更新”页签，界面如下图所示。

系统升级 重启 健康记录 诊断 服务更新			
病毒防御			
病毒库记录数			[更新]
最新更新时间			
许可证到期时间			[更新]
入侵防御			
规则库记录数	2378		[更新]
自定义规则数	0		[导入规则] [导出规则]
最新更新时间			
许可证到期时间			
应用识别			
规则库记录数	129		[更新]
最新更新时间	从未更新		
许可证到期时间	永不过期		
WEB过滤			
URL库记录数	0		[更新]
最新更新时间			
许可证到期时间	Expired		

2) 更新病毒库

点击“病毒库记录数”右侧的“更新”按钮，弹出如下图所示界面：



病毒库有在线升级和离线升级两种方式：

➤ 离线升级

病毒库的离线升级通过在 Web 界面中指定病毒库文件进行，具体操作为：点击“指定病毒库文件”右侧的“浏览...”按钮，选择病毒库文件。然后点击“更新病毒库”按钮，即可完成病毒库的离线升级。如果病毒库升级包选择错误，系统将弹出错误提示框。

也可以在 CLI 命令行中通过位于 TFTP 服务器上的离线升级包进行，关于升级命令的详细说明和具体应用请参见《命令行手册——防病毒配置》。

➤ 在线升级

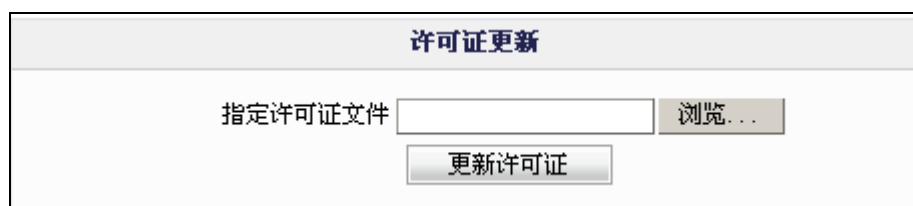
设备连接“服务器地址”处设置的远程病毒库服务器，按照“每日更新时间”设定的时间自动完成升级，或者点击“更新”按钮即时对病毒库进行升级。

说明

- ✧ 升级服务器地址在默认出厂配置中已经设置完成，建议用户不要修改，否则可能会导致无法进行升级操作。
- ✧ 升级服务器地址应为完整的URL，即包括协议前缀，如http://avse.topsec.com.cn。

3) 更新许可证

点击“许可证到期时间”右侧的“更新”按钮，可以更新病毒库许可证，界面如下图所示。



点击“浏览”选择许可证文件后，点击“更新许可证”即可完成许可证更新。

4.3.6.2 更新入侵防御规则库

网络卫士安全网关基于入侵防御规则库对传输的数据包进行检测，检测出内在的攻击行为。系统提供 IPS 规则库的更新和导入导出操作。

入侵防御规则库设置界面如下图：

入侵防御		
规则库记录数	2378	[更新]
自定义规则数	0	[导入规则] [导出规则]
最新更新时间		
许可证到期时间		

管理员可以查看规则库版本、规则库记录数及最新更新时间等信息。

1) 更新规则库

a) 点击“规则库版本”右侧的“更新”按钮，弹出如下图所示窗口。

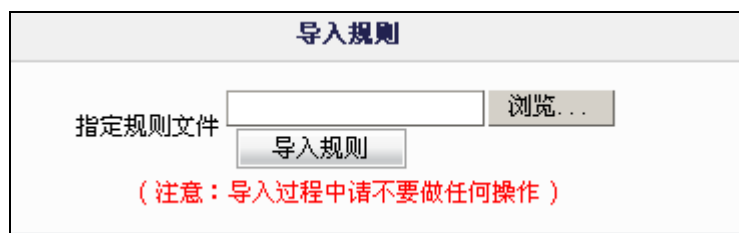
本地更新	
攻击检测规则库	浏览... 更新
远程更新	
自动更新	☒
服务器选择	TOPSEC服务器
每周更新时间	星期日 23 时 59 分
应用 立即更新	

b) 在“本地更新”处，点击“浏览”选择更新文件，然后点击“更新”即可完成对系统规则库的本地更新（该操作需事先通过天融信网站获取更新文件）。

c) 在“远程更新”处，选择是否开启自动更新开关，填入服务器地址及每周、每日更新时间，点击“应用”即可完成定时更新的设定；点击“立即更新”可对系统规则库进行即时更新。

2) 导入自定义规则

点击“导入规则”，弹出如下图所示界面，管理员可以导入自定义的规则。



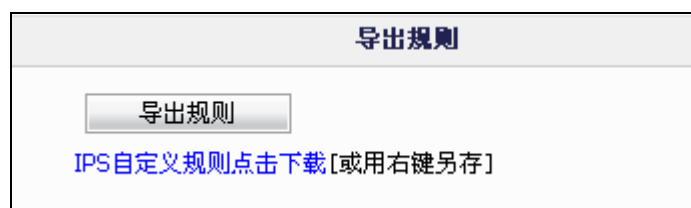
点击“浏览”，选择需要导入的规则文件，然后点击“导入规则”即可完成自定义规则文件的导入操作。

3) 导出规则

点击“导出规则”，弹出如下图所示界面。



点击“导出规则”按钮，如下图所示。



点击此链接或通过鼠标右键菜单选择“目标另存为”，管理员可以将自定义规则保存到管理主机本地的文件夹中。

4.3.6.3 更新应用识别规则库

网络卫士安全网关基于应用识别规则库对应用层数据进行识别，进而根据应用识别策略对数据包进行处理。系统提供应用识别规则库的更新操作。

应用识别规则库设置界面如下图：

应用识别		
规则库记录数	129	[更新]
最新更新时间	从未更新	
许可证到期时间	永不过期	

管理员可以查看规则库记录数及最新更新时间、许可证到期时间等信息。

1) 点击“规则库记录数”右侧的“更新”按钮，可以更新规则库。弹出如下图所示窗口。

本地更新	
应用识别规则库	浏览... 更新
远程更新	
自动更新	☒
服务器选择	TOPSEC服务器 ▼
每周更新时间	星期日 ▼ 23 时 59 分
应用 立即更新	

2) 手动更新规则库

在“本地更新”处，点击“浏览”选择更新文件，然后点击“更新”即可完成对系统规则库的手动更新。更新文件可以在天融信网站获取。

3) 自动更新规则库

在“远程更新”处，选择是否开启自动更新开关，在“服务器选择”栏设置更新服务器，可以选择“TOPSEC 服务器”或者“指定服务器”自行设定；在“每周更新时间”栏设置每周更新时间。参数设置完成后，点击“应用”即可完成定时更新的设定；点击“立即更新”可对系统规则库进行即时更新。

4.3.6.4 更新 URL 库

网络卫士安全网关进行恶意网站过滤时，通过将网站 URL 与保存在设备上的 URL 库进行对比来确定是否为恶意网站，进而根据设定的策略进行 WEB 过滤。设备的 URL 库保存了每一类网站中包含的具体网站名单，为了使 URL 库保持最新的状态，网络卫士安全网关提供 URL 库的更新功能。设备提供两种更新方式：

- 在线更新：直接连接天融信公司提供的 URL 库服务器，在线更新 URL 库信息；
- 手工更新：管理员手工导入最新的 URL 库文件更新 URL 库；

URL 库的升级界面如下所示：

WEB过滤	
URL库记录数	0 [更新]
最新更新时间	
许可证到期时间	Expired

“URL 库记录数”显示设备当前的 URL 库中有多少条 URL 信息；

“最新更新时间”显示 URL 库最近一次更新的时间；

“许可证到期时间”显示 URL 库的许可证到期时间。

1) 更新 URL 库

点击“更新”按钮进入“URL 库更新”页面，如下图所示。

本地更新	
URL库文件名	浏览... 更新

远程更新	
服务器地址	http://webfilter.topsec.com.cn (IP或域名,域名格式http://*)
每日更新时间	00 : 00 [时:分]
应用 立即更新	

2) 手工更新 URL 库

a) 点击“URL 库文件名”右侧的“浏览...”按钮，进入选择 URL 库文件的窗口。

b) 在“选择文件”窗口中选择待更新的 URL 库文件后，点击“打开”按钮，该文件的路径显示在文本框中。

c) 点击“更新”按钮，即可完成 URL 库的离线升级，升级成功后系统会有成功提示信息。如果选择了错误的 URL 库升级包，系统将弹出错误提示框。

3) 在线更新恶意库，指的是通过连接 URL 库服务器来更新 URL 库。

升级所用的“服务器地址”在默认出厂配置中已经设置完成，建议用户不要修改，否则可能会导致无法进行升级操作。

a) 定时更新

管理员只需要设定“每日更新时间”，然后单击“应用”按钮。此后，设备的 URL 库会每天在设定的时间自动完成升级。

b) 手动即时更新

只需点击“立即更新”按钮，便可完成 URL 库的手动即时升级。

4.4 配置系统管理员

网络卫士安全网关支持多个管理员对其进行管理操作，不同的管理员可以设置不同的操作权限。出厂配置中，系统中的管理员分成四种不同的权限，按照 VSID 可以分为两类：根系统管理员（包括：superman、管理用户以及审计用户）和虚拟系统管理员。

a) **根系统管理员**对配置信息具有全局权限，可以看到所有跟该权限对应的公共界面元素和所有虚系统的配置信息。其中，**superman**为系统中唯一的超级管理员，具有网络

卫士安全网关中所有的管理权限；**管理用户**具有查看和设定规则的权限，以及部分安全网关管理权限，但没有分配管理员的权限；**审计用户**能查看已有的规则和配置，但没有管理权限。

b) **虚拟系统管理员**不具备全局权限，只能查看、配置有限的公共信息和本虚拟系统的配置信息。

超级管理员能够根据实际需要配置新的管理权限，并配置系统管理员账号及管理权限。

4.4.1 配置管理员账号

只有超级管理员具有配置系统管理员账号的权力，其他类型的管理员登录系统后只能修改自身的登录密码，左侧导航树中的相应节点变更为 **系统管理 > 修改密码**。

superman配置系统管理员的操作描述如下：

1) 在左侧导航菜单中选择 **系统管理 > 管理员**，界面如下图所示。

管理员						
+ 添加						
用户名	权限	描述	修改密码	修改属性	删除	状态
superman	超级管理员	SuperManager				
aaa	安全管理	NoComment				
gradeadmin	分级管理用户	NoComment				

界面中显示已经配置的管理员信息。其中 **superman** 为系统出厂时配置的超级管理员，以 **superman** 身份登录安全网关后，只能修改超级管理员的密码及其他属性，不能删除 **superman**。

2) 添加管理员。

a) 点击“添加”，进入“添加用户”界面，如下图所示。

添加用户

用户名称

*

用户描述

用户密码

*

确认密码

*

用户权限

管理用户

（提示：口令最小长度 8）

确定

取消

界面参数说明如下表所示。

参数	说明
用户名称	指管理员的用户名称。不能超过 31 个字符，一个汉字相当于两个字符。
用户描述	指管理员的相关描述。
用户密码	指管理员的用户密码，密码的设定只要满足 系统管理 > 管理员 的“设置”中设置的“口令策略”即可。 如果管理员在 系统管理 > 管理员 的“设置”中设置了“口令策略”，则用户密码的设定必须符合已经设定的口令安全机制。例如，口令强度设置为“中”，则设置的口令中必须至少包含一个小写字母。
确认密码	再次输入管理员的用户密码。 最少不能低于 8 位。
用户权限	设置管理员的权限。 可选值为：管理用户、审计用户、虚拟系统用户、分级管理用户，以及超级管理员在“管理权限”处设置的其他管理权限。 说明： 1) 管理用户是指对网络卫士安全网关具有管理权限（但不能修改管理员配置）的用户； 2) 审计用户只有查看配置的权限，不能修改配置；虚系统用户则只能登录网络卫士安全网关上指定的虚系统。 3) 分级管理用户登录安全网关后，只具备查看其所属角色、修改由他创建的用户权限，分级管理员所创建的用户均属于该管理员对应的角色。为分级管理员分配角色请参见 8.2.2 分级管理 。 4) 选择具体的“管理权限”后将具有权限对象设置的管理权限，具体设置请参见 4.4.2 配置管理权限 。
虚拟系统号	只有当“用户权限”设定为“虚拟系统用户”时显示该项，用于设定管理员所属的虚拟系统号。 取值范围：1-254。

b) 参数设置完成后，点击“确定”按钮，完成管理员账号的添加；点击“取消”按钮，取消此次操作。

3) 修改管理员属性

点击指定管理员后面的“修改密码”图标，可以修改该管理员的登录密码。

点击指定管理员后面的“修改属性”图标，可以修改该管理员的描述信息，或修改其管理权限。

4) 启用或禁用管理员

点击指定管理员“状态”一系列的图标，可以“启用”或“禁用”该管理员，禁用后将使得该管理员无效。

5) 删除管理员

只能删除 Superman 以外的其他账号。

点击指定管理员后面的“删除”图标，可以删除该管理员账号。

4.4.2 配置管理权限

网络卫士安全网关基于管理权限对 **superman** 以外的管理员进行权限控制。出厂配置中，系统中的管理员分成三种不同的管理权限：管理用户、审计用户、虚拟系统管理员和分级管理员。

通过配置管理权限，将网络卫士安全网关设备的一些功能划分为不同的访问控制类型，对不同的访问控制类型都可以分别设置具有读或写的权限。读的权限是指管理员能够查看基于 **web** 的管理器的页面中的功能选项。管理员只有具备写的权限才可以更改页面中的设置。

管理员在此对管理权限进行管理和设置，包括新管理权限添加，已有的管理权限信息的编辑、删除、查找、清空等。还可以设置具有某种管理权限的管理员信息。

具体步骤描述如下：

1) 在左侧导航菜单中选择 **系统管理 > 管理员**，并激活“管理权限”页签，进入管理员角色配置界面。

管理员 管理权限 设置			
+ 添加 清空			
模板名称	模板描述	修改	删除

2) 添加管理员角色。

a) 点击“添加”，进入设置界面，如下图所示。

新建权限模板

模板名称 *

模板描述

功能模块	□ 无	□ 只读	□ 读写
系统设置	☒	☐	☐
系统维护	☒	☐	☐
网络管理	☒	☐	☐
资源管理	☒	☐	☐
用户认证	☒	☐	☐
安全策略	☒	☐	☐
深度内容过滤	☒	☐	☐
PKI	☒	☐	☐
虚拟专网	☒	☐	☐
SSLVPN模块	☒	☐	☐
入侵防御	☒	☐	☐
病毒防御	☒	☐	☐
反垃圾邮件	☒	☐	☐
高可用性	☒	☐	☐
日志设置	☒	☐	☐
日志访问	☒	☐	☐

界面参数说明如下表所示。

参数	说明
模板名称	输入对象名称。
模板描述	输入对象必要的描述信息，为可选项。
功能模块	显示可以设置访问权限的功能选项。所有管理员均具有查看系统“基本信息”、“系统监视”信息和“修改自身登录密码”的功能。勾选相应模块的“只读”，则具有查看该模块相关配置的功能；如果勾选相应模块的“读写”，则管理员具有查看及配置该模块相关菜单的功能；勾选“无”，表示不具有该模块的设置及查看权限。具体说明为： 系统设置：设置是否具有 系统管理 > 配置 菜单的相关配置权限。 系统维护：设置是否具有 系统管理 > 连接信息、维护 菜单的相关配置权限。 网络管理：设置是否具有“网络管理”模块的配置权限。 资源管理：设置是否具有“资源管理”模块的配置权限。 用户认证：设置是否具有“用户认证”模块的配置权限。 安全策略：设置是否具有“防火墙”模块的配置权限。 深度内容过滤：设置是否具有“内容过滤”模块、“应用识别”模块的配置权限。

参数	说明
	PKI 模块：设置是否具有“PKI”模块的配置权限。 虚拟专网：设置是否具有“虚拟专网”模块的配置权限。 SSLVPN 模块：设置是否具有“SSL VPN”模块的配置权限。 入侵防御：设置是否具有“入侵防御”模块的配置权限。 病毒模块：设置是否具有“病毒防御”模块的配置权限。 反垃圾邮件：设置是否具有“反垃圾邮件”模块的配置权限。 高可用性：设置是否具有“高可用性”模块的配置权限。 日志设置：设置是否具有“日志设置”模块的配置权限。 日志访问：设置是否具有“日志查看”模块的配置权限。
无	勾选“无”，表示不具有该模块的设置及查看权限。
只读	勾选“只读”，表示具有查看该模块设置的权限。
读写	勾选“读写”，表示具有该模块的查看及设置的所有权限。

b) 参数设置完成后，点击“确定”按钮，完成管理权限的添加；点击“取消”按钮，取消此次操作。

3) 修改管理权限对象的属性

点击指定对象后面的“修改”图标，可以修改该对象的属性。

4) 删除管理权限对象

点击指定对象后面的“删除”图标，可以删除该对象。

点击“清空”，将一次性删除所有的对象。

4.4.3 设置

管理员负责安全网关的管理与配置，因此为保证网络卫士安全网关的安全性，管理员的登录会话必须设置一定的安全保护机制。网络卫士安全网关可以通过设置管理会话超时、管理员的最大并发管理数、同一用户最大并发管理数、最大登录失败次数等，提高管理员管理设备的安全性。

具体设置为：

1) 在左侧导航菜单中选择 **系统管理 > 管理员**，并激活“设置”页签，进入管理安全配置界面。

设置

管理员设置

WEB管理超时 [30-3600秒或0表示永超时]

最大并发管理数 * [不大于64个]

同一用户最大并发管理数 * [不大于32个]

最大登录失败次数 * [不大于5次]

口令策略

口令强度

口令最小长度 * [8-31]

参数说明如下表所示：

参数	说明
WEB 管理超时时间	设定利用 WEBUI 界面对安全网关进行管理的空闲超时时间。范围为 30-3600 秒。默认值为 180 秒，设置为 0，表示永超时。
最大并发管理数目	当最大并发管理数目为 N 时，允许 N 个不同名管理员同时登录到设备。默认值为 5，范围 1-64。
同一用户最大并发管理数	设定使用同一管理员名可以同时登录设备的最大次数。默认值为 5，范围 1-32。
最大登录失败次数	设定登录失败时，允许同名用户尝试登录的最多次数，超过该次数则被锁定。默认锁定 1 分钟，可以通过命令行方式修改。用户可以再次尝试登录。默认值为 5，范围 1-5 次。
口令强度	设置添加管理员时口令强度的强弱程度。可选项为：弱、中、强。 说明： 设置为“弱”时，只有口令长度的限制，没有口令复杂度限制； 设置为“中”时，有口令长度限制，且口令复杂度为：至少包含一个数字和至少包含一个小写字母； 设置为“强”时，有口令长度限制，且口令复杂度为：至少包含一个数字，至少包含一个小写字母，至少包含一个大写字母，而且至少包含一个数字和字母外的其他符号，且口令中不能包含用户名。
口令最小长度	设置添加管理员时口令的最小长度。范围为 8-31。

设置完成后，点击“应用”按钮保存设置。

5 系统监视

网络卫士安全网关提供了深度统计功能，支持对系统总体及某一特定对象（如基于接口、协议、内容或其他规则）通信量、连接数、病毒攻击、应用流量、带宽等数据的采集、统计和显示，用以满足用户对各种数据统计以及应用层流量管理需求。

5.1 连接信息

连接信息指的是当前通过安全网关建立的连接信息。

1) 选择 **系统监视 > 连接信息**，管理员可以查看当前时刻通过安全网关建立的连接信息，如下图所示。

连接信息								
协议	全部	源IP		源端口		目的IP		目的端口
清空连接表								总计: 8
连接状态: 连接 断开 握手 *长连接					☐ 服务名		删除	
状态	协议	源IP:端口	源NAT IP:端口	RX	目的IP:端口	目的NAT IP:端口	TX	
	tcp	192.168.83.224:3162	192.168.83.224:3162	7	192.168.83.233:8080	192.168.83.233:8080	8	☐
	tcp	192.168.83.224:3160	192.168.83.224:3160	8	192.168.83.233:8080	192.168.83.233:8080	8	☐
	tcp	192.168.1.2:3568	192.168.1.2:3568	7	192.168.1.3:443	192.168.1.3:443	7	☐
	tcp	192.168.1.2:3567	192.168.1.2:3567	7	192.168.1.3:443	192.168.1.3:443	7	☐
	tcp	192.168.1.2:3566	192.168.1.2:3566	7	192.168.1.3:443	192.168.1.3:443	7	☐
	tcp	192.168.1.2:3565	192.168.1.2:3565	4	192.168.1.3:443	192.168.1.3:443	2	☐
	tcp	12.12.12.30:3564	192.168.83.233:3564	4	192.168.83.235:80	192.168.83.235:80	3	☐
	tcp	192.168.1.2:3534	192.168.1.2:3534	12	192.168.1.3:443	192.168.1.3:443	15	☐

每一条连接信息包括的内容说明如下表所示：

参数	说明
状态	显示该连接的状态：不同的图标分别表示不同的状态信息。图标的具体含义可以在“状态缩写”处查看。
协议	显示该连接所使用的协议，为 TCP、UDP、ICMP；
源 IP：端口	显示该连接的源 IP 地址及端口号。
源 NAT IP：端口	显示该连接的源 IP 地址及端口号是否经过 SNAT 转换。
RX	显示该连接建立过程中源地址发送的数据报文个数。
目的 IP：端口	显示该连接的目的 IP 地址及端口号。
目的 NAT IP：端口	显示该连接的目的 IP 地址及端口号是否经过 DNAT 转换。
TX	该连接建立过程中目的地址发送的数据报文个数。

a) 点击“刷新”按钮可以在界面显示最新的连接信息。

b) 查找连接信息

在“源 IP”、“源端口”、“目的 IP”、“目的端口”和“协议”处可以输入一个或多个查询参数，并点击“查找”按钮，则在下面会显示查询的结果信息。当输入多个查询参数时，同时满足这些条件的连接信息才会显示在列表中。

c) 删除连接

点击某条连接信息对应的“删除”图标删除该条连接信息。点击“清空连接表”一次性删除所有的连接信息。

d) 勾选“服务名”，可以实现对目的端口的识别功能，对常见知名端口翻译为对应的协议，如下图所示。

连接信息									
协议	全部	源IP		源端口		目的IP		目的端口	
清空连接表								查找	刷新
连接状态: 连接 断开 握手 #长连接								总计: 3	
								☒ 服务名	删除
状态	协议	源IP:端口	源NAT IP:端口	RX	目的IP:端口	目的NAT IP:端口	TX		
	tcp	192.168.83.224:3997	192.168.83.224:3997	5	192.168.83.237:8080	192.168.83.237:8080	5	☐	
	tcp	192.168.83.224:3995	192.168.83.224:3995	7	192.168.83.237:8080	192.168.83.237:8080	8	☐	
	udp	192.168.83.237:500	192.168.83.237:500	1409	192.168.83.233:IPSEC_ISAKMP	192.168.83.233:IPSEC_ISAKMP	0	☐	

5.2 接口流量

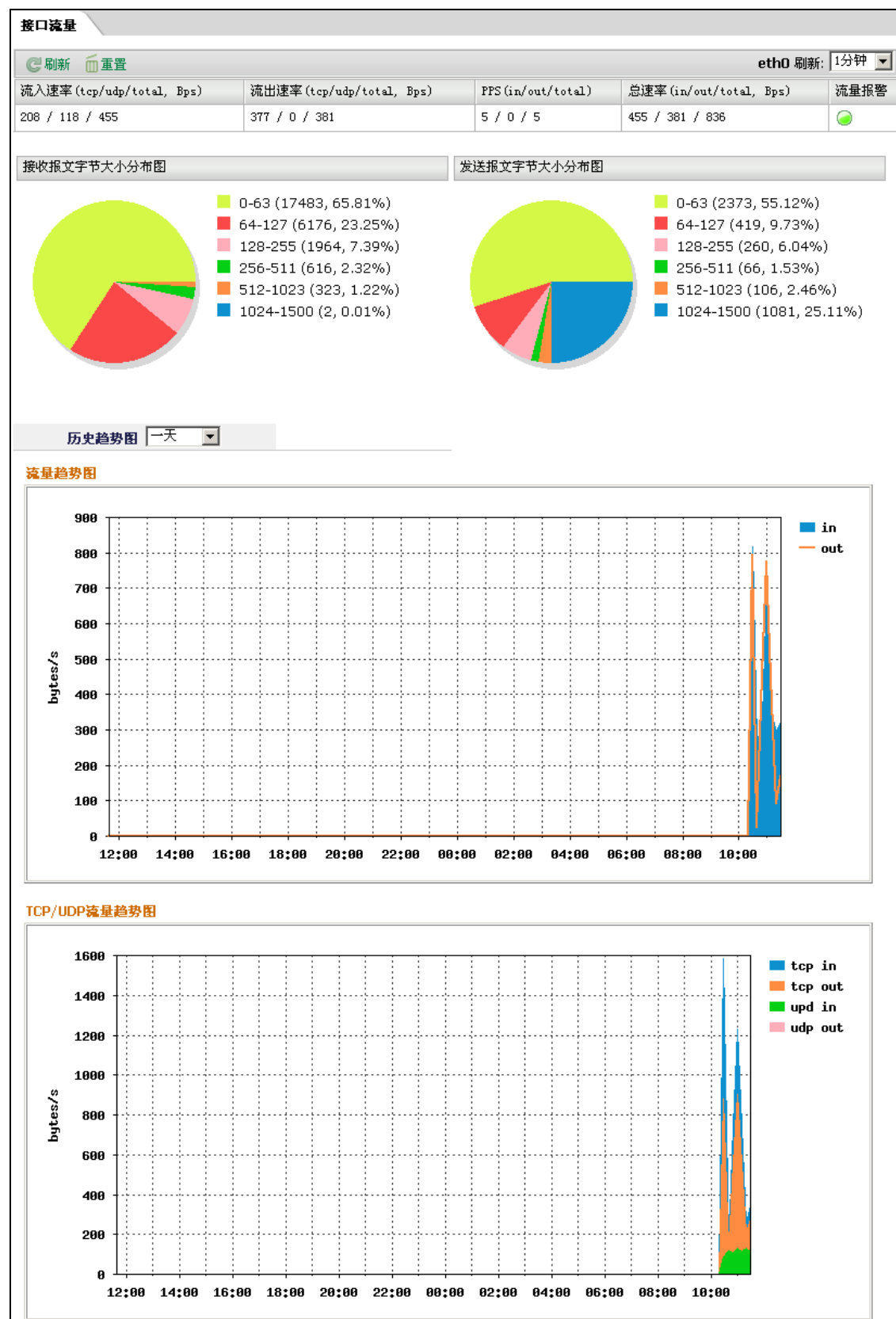
网络卫士安全网关支持对通过设备的数据报文流量进行统计。根据安全网关的物理接口，对通过该接口的数据流量进行统计，主要包括发送、接收的总流量统计和速率统计。

1) 选择 **系统监视 > 接口流量**，界面将会显示安全网关所有物理接口的流量统计信息。如下图所示。

接口流量				
接口	总流量		速率	
	接收字节	发送字节	接收bps	发送bps
eth0	1,527,219	1,888,031	16K	112
eth1	1,061,313	4,355,696	368	0
eth2	0	0	0	0
eth3	0	0	0	0
veth0.01	0	0	0	0

页面中显示了各个物理接口接收、发送的总流量以及接收、发送实时速率的统计情况。

2) 点击具体接口，显示该接口的详细流量信息，如下图所示。



页面上方显示了该接口流入/流出速率、流量报警状态以及接收/发送报文字节饼图。

页面下方显示了该接口的流量趋势图和 TCP/UDP 流量趋势图。点击“历史趋势图”右侧的下拉框选择统计周期，包括：一天、一周和一月。

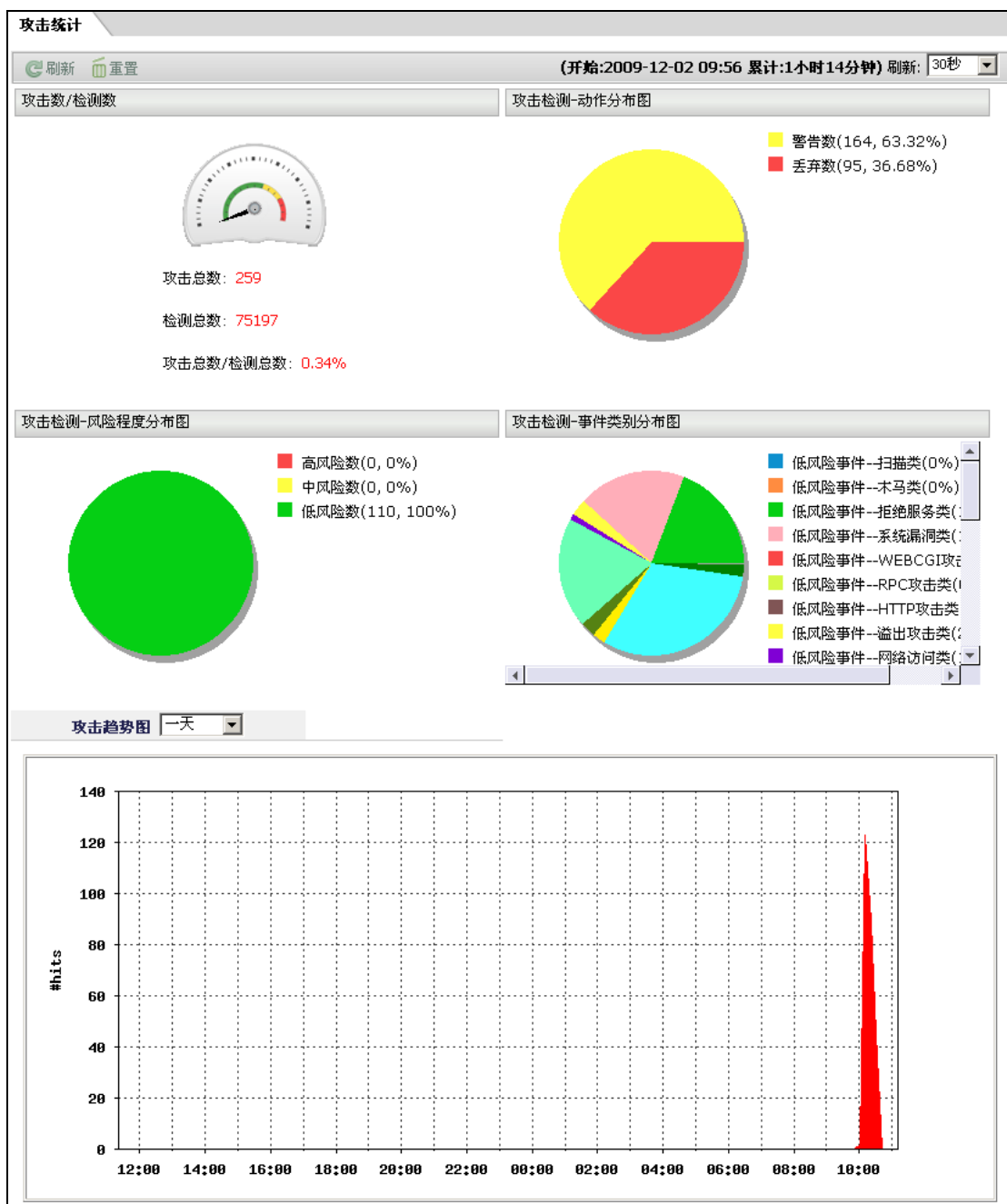
在页面右上角的“刷新”栏内设定刷新周期，可选项包括：10 秒、30 秒、1 分钟、10 分钟和不刷新；点击“刷新”，界面中显示系统当前的统计信息。

5.3 攻击统计

针对于检测到的攻击、事件类型、风险程度以及系统对攻击所执行的操作,网络卫士安全网关在采集这些信息的基础上给出了攻击数/检测数、攻击检测-动作分布图、攻击检测-风险程度分布图、攻击检测-事件类别分布图以及攻击趋势图。

1) 查看攻击统计

选择 系统监视 > 攻击统计，如下图所示。



“攻击数/检测数”图可以查看到系统实时检测到的统计开始时间、攻击数、检测数以及攻击数与检测数的百分比。注：表盘刻度表示攻击检测百分比，量程为 0%-100%。

“攻击检测-动作分布图”可查看当前系统对匹配到攻击检测规则的报文分别执行警告和丢弃的统计量及其百分比。

“攻击检测-风险程度分布图”可以查看当前系统对于匹配到攻击检测规则的事件中，高中低三类事件的百分比。

“攻击检测-事件类别分布图”可以查看在系统入侵防御规则库事件分类的基础上，命中不同类型事件的百分比。

“攻击趋势图”则给出了一天、一周、一月不同的时间点或时间段内受到攻击数的统计趋势。在“攻击趋势图”右侧的下拉框内可以选择攻击趋势图的统计周期，可选项包括：一天、一周和一月。

2) 刷新攻击统计

在页面右上角“刷新”栏内设定刷新周期，可选项包括：10 秒、30 秒、1 分钟、10 分钟和不刷新；点击“刷新”刷新当前页面。

5.4 攻击排名

根据系统检测到的攻击统计，网络卫士安全网关可以对攻击事件和受攻击的主机进行排名。

5.4.1 攻击排名

按照攻击次数排名，系统列出了从“开始”时间算起的全部攻击事件及事件本身的详细内容，包括：排名、事件号、级别、次数及事件描述。

1) 查看攻击排名

选择 **系统监视 > 攻击排名**，选择“攻击排名”页签，进入“攻击排名”页面，如下图所示。

攻击排名		受攻击主机排名		
刷新 重置		(开始:2009-12-02 09:56 累计:1小时15分钟) 排序: 攻击总数 刷新: 30秒		
排名	事件号	级别	次数	事件描述
1	12200	低	50	3cdaemon 拒绝服务攻击
2	12628	低	50	Avaya Hidden Community String 攻击
3	12641	高	50	D-Link Internet Camera 拒绝服务攻击
4	12617	中	50	3Com TFTP 3CDaemon拒绝服务攻击
5	12633	高	24	Breed Empty UDP 拒绝服务攻击
6	12645	高	2	IBM Lotus Domino LDAP 服务内存异常攻击
7	12646	高	2	IBM Tivoli Directory Server Unspecified LDAP内存破坏漏洞攻击
8	12644	低	2	IBM Lotus Domino LDAP 服务无效消息溢出攻击
9	12247	高	2	潜入者 木马连接操作
10	12631	高	2	Tcpdump BGP 内存无效数据拒绝服务攻击
11	12392	高	2	CMD版灰鸽子 木马连接操作

“开始时间”为统计攻击排名的起始时间，清空攻击排名后，开始时间将被重置。

在“排序”栏选择排序关键字可以将攻击事件按照关键字进行排序，可选项包括：攻击总数和高风险。

点击事件号可以查看该事件的详细信息。

2) 刷新攻击排名

在“刷新”栏内设定刷新周期，可选项包括：10 秒、30 秒、1 分钟、10 分钟和不刷新；点击页面左上角的“刷新”，界面中显示系统当前的攻击排名及其详细信息。

3) 清空攻击排名

点击页面左上角的“重置”清空统计数据，同时统计开始时间也会被重置。

5.4.2 受攻击主机排名

根据攻击统计信息，系统可以显示从“开始”时间算起的受到攻击的全部监控主机排名。关于监控主机的设置具体请参见 [11.3主机监控](#)。

1) 查看受攻击主机排名

选择 **系统监视 > 攻击排名**，选择“受攻击主机排名”页签，进入“受攻击主机排名”页面，如下图所示。

攻击排名		受攻击主机排名	
刷新 重置		(开始:2010-08-02 07:56 累计:1小时56分钟) 刷新: 30秒	
主机IP	高风险	一般风险	低风险
58.254.39.12	0	0	6
58.251.62.25	0	0	6
60.172.222.8	0	0	2
58.60.15.31	0	0	3
219.133.60.243	0	0	65
60.172.222.5	0	0	7
172.16.164.44	0	0	1

“开始时间”为统计攻击排名的起始时间，清空攻击排名后，开始时间将被重置。

管理员可以通过点击“主机 IP”、“高风险”、“一般风险”和“低风险”右侧的升序/降序箭头来对受监控的主机进行相应关键字的排序。上图中即为按照主机受到高风险事件攻击次数的降序排名。

点击主机 IP 可以查看该主机所受攻击的详细信息，如下图所示。

攻击排名

受攻击主机排名

刷新重置

(开始:2010-08-02 07:56 累计:1小时56分钟) 刷新: 30秒

主机IP

58.254.39.12

58.251.62.25

60.172.222.8

58.60.15.31

219.133.60.243

60.172.222.5

172.16.164.44

编号

规则名称

风险程度

统计

12030

P2P软件 迅雷 资源查询操作

低风险

8

2) 刷新受攻击主机排名

在“刷新”栏内设定刷新周期，可选项包括：10 秒、30 秒、1 分钟、10 分钟和不刷新；点击页面左上角的“刷新”，界面中显示系统当前的排名及其详细信息。

3) 清空受攻击主机排名

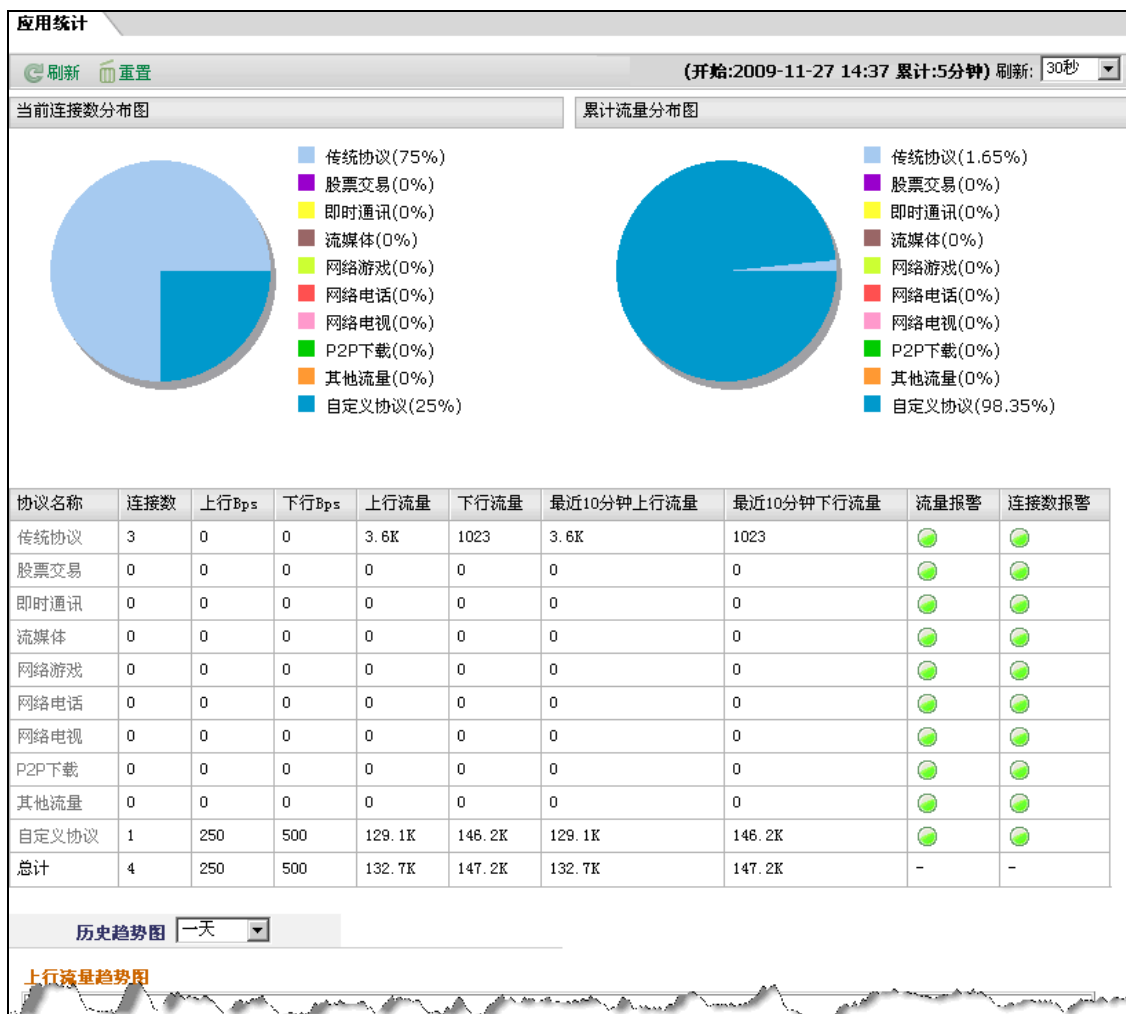
点击页面左上角的“重置”清空统计数据，同时统计开始时间也会被重置。

5.5 应用统计

应用统计主要是对每种应用协议的连接数和上下行流量进行了统计，方便用户掌握系统大流量应用的动向并对其及时采取控制操作。网络卫士安全网关检测识别的应用协议包括：传统协议、股票交易、即时通讯、流媒体、网络游戏、网络电话、P2P 下载、其他流量以及自定义协议。

1) 查看应用统计

选择 **系统监视** > **应用统计**，如下图所示。



“开始时间”为应用统计的起始时间，清空统计后，开始时间将被重置。

页面上方显示了基于应用协议的当前连接数分布图、累计流量分布图以及各应用协议的连接数/流量统计列表。应用协议统计信息列表除了显示了各应用协议的连接数和流量信息，还显示了连接数和流量的报警信息，其中红色表示有报警，绿色表示没有报警。关于流量和连接数报警阈值的设置具体请参见[11.5流量异常检测](#)；点击协议名称可以查看该协议详细的统计信息。

页面下方显示了各应用协议上下行流量和连接数的历史趋势图。点击“历史趋势图”右侧的下拉框选择统计周期，包括：一天、一周和一月。

2) 刷新应用统计

在“刷新”栏内设定刷新周期，可选项包括：10秒、30秒、1分钟、10分钟和不刷新；点击页面左上角的“刷新”，界面中显示系统当前的统计信息。

3) 清空应用统计

点击页面左上角的“重置”清空统计数据，同时统计开始时间也会被重置。

5.5.1 传统协议

1) 查看传统协议流量统计

选择 **系统监视 > 应用统计**，在“协议名称”列表中点击“传统协议”，如下图所示。



页面上方显示了各传统协议的连接数/流量统计列表；点击协议名称可以查看该协议的详细统计信息。

页面下方显示了传统协议总体的流量趋势图和连接趋势图。点击“历史趋势图”右侧的下拉框选择统计周期，可选项包括：一天、一周和一月。

2) 刷新传统协议统计

在“刷新”栏内设定刷新周期，可选项包括：10 秒、30 秒、1 分钟、10 分钟和不刷新；点击“刷新”，界面中显示系统当前的统计信息。

5.5.2 股票交易

选择 **系统监视 > 应用统计**，在“协议名称”列表中点击“股票交易”，如下图所示。

应用统计							
刷新		股票交易 刷新: 30秒					
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量	最近10分钟上行流量	最近10分钟下行流量
同花顺	0	0	0	0	0	0	0
大智慧	0	0	0	0	0	0	0
钱龙	0	0	0	0	0	0	0
天下无双	0	0	0	0	0	0	0
广发至强交易系统	0	0	0	0	0	0	0
飞狐交易师	0	0	0	0	0	0	0
指南针金融系统	0	0	0	0	0	0	0
安信行情	0	0	0	0	0	0	0
分析家	0	0	0	0	0	0	0
和讯股道	0	0	0	0	0	0	0
任家信	0	0	0	0	0	0	0
文华财经	0	0	0	0	0	0	0
银河证券	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0

历史趋势图 一天

股票交易类应用统计的操作与传统协议类似，具体请参见[5.5.1传统协议](#)。

5.5.3 即时通讯

选择 **系统监视** > **应用统计**，在“协议名称”列表中点击“即时通讯”，如下图所示。

应用统计							
刷新		即时通讯 刷新: 30秒					
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量	最近10分钟上行流量	最近10分钟下行流量
QQ登录	0	0	0	0	0	0	0
QQ文件传输	0	0	0	0	0	0	0
QQ语音视频聊天	0	0	0	0	0	0	0
MSN登录	0	0	0	0	0	0	0
MSN语音视频聊天	0	0	0	0	0	0	0
MSN文件传输	0	0	0	0	0	0	0
淘宝网旺旺登录	0	0	0	0	0	0	0
阿里旺旺登录	0	0	0	0	0	0	0
YahooMessenger登录	0	0	0	0	0	0	0
YahooMessenger语音聊天	0	0	0	0	0	0	0
YahooMessenger文件传输	0	0	0	0	0	0	0
新浪UC登录	0	0	0	0	0	0	0

即时通讯类应用统计的操作与传统协议类似，具体请参见[5.5.1传统协议](#)。

5.5.4 流媒体

选择 **系统监视** > **应用统计**，在“协议名称”列表中点击“流媒体”，如下图所示。

应用统计							
刷新		流媒体 刷新: 30秒					
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量	最近10分钟上行流量	最近10分钟下行流量
Web视频	0	0	0	0	0	0	0
飞速土豆	0	0	0	0	0	0	0
PP加速器	0	0	0	0	0	0	0
新浪视频	0	0	0	0	0	0	0
新传体育	0	0	0	0	0	0	0
央视网	0	0	0	0	0	0	0
QuickTime	0	0	0	0	0	0	0
RTSP	0	0	0	0	0	0	0
RealPlayer	0	0	0	0	0	0	0
MMS	0	0	0	0	0	0	0
皮皮影视	0	0	0	0	0	0	0
FastTv	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0

历史趋势图 一天

流媒体类应用统计的操作与传统协议类似，具体请参见[5.5.1传统协议](#)。

5.5.5 网络游戏

选择 **系统监视 > 应用统计**，在“协议名称”列表中点击“网络游戏”，如下图所示。

应用统计							
刷新		网络游戏 刷新: 30秒					
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量	最近10分钟上行流量	最近10分钟下行流量
QQ游戏	0	0	0	0	0	0	0
跑跑卡丁车	0	0	0	0	0	0	0
QQ音速	0	0	0	0	0	0	0
QQ三国	0	0	0	0	0	0	0
QQ幻想	0	0	0	0	0	0	0
梦幻西游	0	0	0	0	0	0	0
联众世界	0	0	0	0	0	0	0
劲舞团	0	0	0	0	0	0	0
面对面	0	0	0	0	0	0	0
泡泡游戏	0	0	0	0	0	0	0
中国游戏中心	0	0	0	0	0	0	0
浩方	0	0	0	0	0	0	0

网络游戏类应用统计的操作与传统协议类似，具体请参见 [5.5.1传统协议](#)。

5.5.6 网络电话

选择 **系统监视 > 应用统计**，在“协议名称”列表中点击“网络电话”，如下图所示。

应用统计							
刷新		网络电话 刷新: 30秒					
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量	最近10分钟上行流量	最近10分钟下行流量
飞线漫游	0	0	0	0	0	0	0
RedVIP	0	0	0	0	0	0	0
ETnano	0	0	0	0	0	0	0
net2phone	0	0	0	0	0	0	0
skype	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0

历史趋势图 一天

网络电话类应用统计的操作与传统协议类似，具体请参见 [5.5.1传统协议](#)。

5.5.7 网络电视

选择 **系统监视** > **应用统计**，在“协议名称”列表中点击“网络电视”，如下图所示。

应用统计							
刷新		网络电视 刷新: 30秒					
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量	最近10分钟上行流量	最近10分钟下行流量
PPStream	0	0	0	0	0	0	0
PPLive	0	0	0	0	0	0	0
QQlive	0	0	0	0	0	0	0
风行	0	0	0	0	0	0	0
UUSee	0	0	0	0	0	0	0
极速酷6	0	0	0	0	0	0	0
TvAnts	0	0	0	0	0	0	0
SopCast	0	0	0	0	0	0	0
PPMATE	0	0	0	0	0	0	0
vgo	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0

历史趋势图 一天

网络电视类应用统计的操作与传统协议类似，具体请参见 [5.5.1传统协议](#)。

5.5.8 P2P 下载

选择 **系统监视** > **应用统计**，在“协议名称”列表中点击“P2P下载”，如下图所示。

应用统计							
刷新		P2P下载 刷新: 30秒					
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量	最近10分钟上行流量	最近10分钟下行流量
BitTorrent	0	0	0	0	0	0	0
迅雷	0	0	0	0	0	0	0
FlashGet	0	0	0	0	0	0	0
超级旋风	0	0	0	0	0	0	0
酷我音乐盒	0	0	0	0	0	0	0
酷狗音乐	0	0	0	0	0	0	0
搜娱	0	0	0	0	0	0	0
eDonkey	0	0	0	0	0	0	0
百宝	0	0	0	0	0	0	0
PP点点通	0	0	0	0	0	0	0
RaySource	0	0	0	0	0	0	0

P2P下载类应用统计的操作与传统协议类似，具体请参见[5.5.1传统协议](#)。

5.5.9 其他流量

选择 **系统监视** > **应用统计**，在“协议名称”列表中点击“其他流量”，如下图所示。

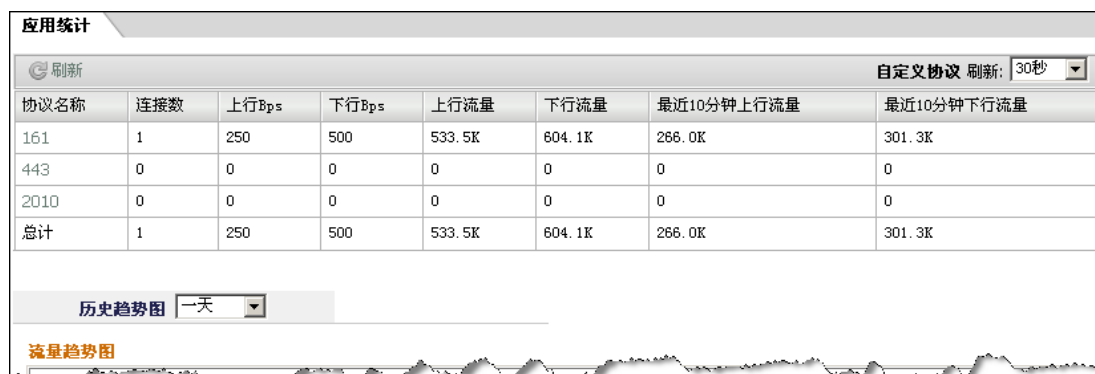
应用统计							
刷新		其他流量 刷新: 30秒					
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量	最近10分钟上行流量	最近10分钟下行流量
未知协议	0	0	0	0	0	0	0
疑似p2p	0	0	0	0	0	0	0
总计	0	0	0	0	0	0	0

历史趋势图 一天

其他流量类应用统计的操作与传统协议类似，具体请参见[5.5.1传统协议](#)。

5.5.10 自定义协议

选择 **系统监视** > **应用统计**，在“协议名称”列表中点击“自定义协议”，如下图所示。



自定义类应用统计的操作与传统协议类似，具体请参见[5.5.1传统协议](#)。

自定义协议的配置操作具体请参见 [11.2自定义应用](#)。

5.6 应用排名

根据系统对应用进行的连接数和流量等的统计信息，网络卫士安全网关可以对具体应用和主机应用进行排名。

5.6.1 应用排名

1) 查看应用排名

选择 **系统监视** > **应用排名**，选择“应用排名”页签，进入“应用排名”页面，如下图所示。

应用排名

应用主机排名

刷新

重置

(开始:2009-11-27 14:37 累计:23分钟) 刷新:

30秒

协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量
161	1	250	500	610.0K	690.8K
HTTP	3	0	0	6.2K	237.5K
POP3	0	0	0	2.4K	36.0K
DNS	1	0	0	14.9K	3.0K
SMTP	0	0	0	42.3K	2.6K
HTTP分块传输	0	0	0	0	0
伪IE下载	0	0	0	0	0
SMB	0	0	0	0	0
TELNET	0	0	0	0	0
SSH	0	0	0	0	0
IMAP	0	0	0	0	0
SSL	0	0	0	0	0
远程桌面	0	0	0	0	0
netbios	0	0	0	0	0
DHCP	0	0	0	0	0

“开始时间”为统计应用排名的起始时间，清空排名后，开始时间将被重置。

管理员可以通过点击“协议名称”、“连接数”、“上行 Bps”、“下行 Bps”、“上行流量”和“下行流量”右侧的升序/降序箭头来对应用进行相应关键字的排序。上图中即为按照应用协议“下行流量”的降序排名。

点击某应用协议名称可以查看是哪些主机占用了该应用协议的上下行流量，如下图所示。

应用排名		应用主机排名			
协议名称	连接数	上行Bps	下行Bps	上行流量	下行流量
161					738.8K
HTTP					237.5K
POP3					36.0K
DNS					3.2K
SMTP					2.6K
HTTP分块传输					0
伪IE下载					0
SMB					0
TELNET					0
SSH					0
IMAP					0
SSL					0
远程桌面					0
netbios					0

IP地址	上次访问	上行流量	下行流量
192.168.98.131	3分钟前	237.5K	6.2K
10.0.0.100	3分钟前	6.2K	237.5K

2) 刷新应用排名

在“刷新”栏内设定刷新周期，可选项包括：10 秒、30 秒、1 分钟、10 分钟和不刷新；点击页面左上角的“刷新”立即刷新页面。

3) 清空应用排名

点击页面左上角的“重置”清空统计数据，同时统计开始时间也会被重置。

5.6.2 应用主机排名

网络卫士安全网关可以对加入主机监控的对象进行应用主机排名，关于监控主机的设置具体请参见 [11.3主机监控](#)。

1) 查看应用主机排名

选择 **系统监视 > 应用排名**，选择“应用主机排名”页签，进入“应用主机排名”页面，如下图所示。

应用排名		应用主机排名			
刷新 重置		2009-11-27 14:37 累计:29分钟) 刷新: 10分钟			
对象名	连接数	上行Bps	下行Bps	上行流量	下行流量
any	2	907	902	2.0M	2.0M
10-100	1	408	462	848.2K	1.2M
98-131	0	0	0	353.5K	58.7K
1-169	0	0	0	314	284
100-1	0	0	0	0	0
110-1	0	0	0	0	0
98-132	0	0	0	0	0
100-100	0	0	0	0	0
12-1	0	0	0	0	0

“开始时间”为统计应用主机排名的起始时间，清空应用排名后，开始时间将被重置。

点击对象名可以查看该对象包含的主机所应用的应用协议流量的详细信息，下图为对象“any”所包含主机的应用排名。

应用排名		应用主机排名			
IP 关键字: 查找		(开始:2009-11-27 14:37 累计:37分钟) 刷新: 10分钟			
刷新 重置					
主机IP	连接数	上行Bps	下行Bps	上行流量	下行流量
10.0.0.100	1	408	462	1.0M	1.4M
192.168.87.178	1	499	440	1.1M	972.7K
192.168.98.131	0	1	1	353.9K	58.9K
100.0.0.2	0	0	0	3.8K	18.5K
192.168.1.169	0	0	0	314	284
12.0.0.1	0	0	0	0	0

在“IP 关键字”栏内输入 IP 地址可查询所关心的主机的应用流量信息。

点击具体的主机 IP 可查看该主机详细的应用协议流量信息，如下图所示。

应用排名		应用主机排名			
IP 关键字: 查找		(开始:2009-11-27 14:37 累计:37分钟) 刷新: 10分钟			
刷新 重置					
主机IP	连接数	协议名	上次访问	上行流量	下行流量
10.0.0.100	1	161	0分钟前	1.1M	1.2M
192.168.87.178	1	HTTP	15分钟前	10.6K	268.2K
192.168.98.131	0	SMTP	32分钟前	42.3K	2.6K
100.0.0.2	0	POP3	3分钟前	6.6K	83.7K
192.168.1.169	0	远程桌面	0分钟前	44.3K	143.3K
12.0.0.1	0	DNS	8分钟前	18.5K	3.8K

2) 刷新应用主机排名

在“刷新”栏内设定刷新周期，可选项包括：10 秒、30 秒、1 分钟、10 分钟和不刷新；点击页面左上角的“刷新”，立即刷新当前页面。

3) 清空应用主机排名

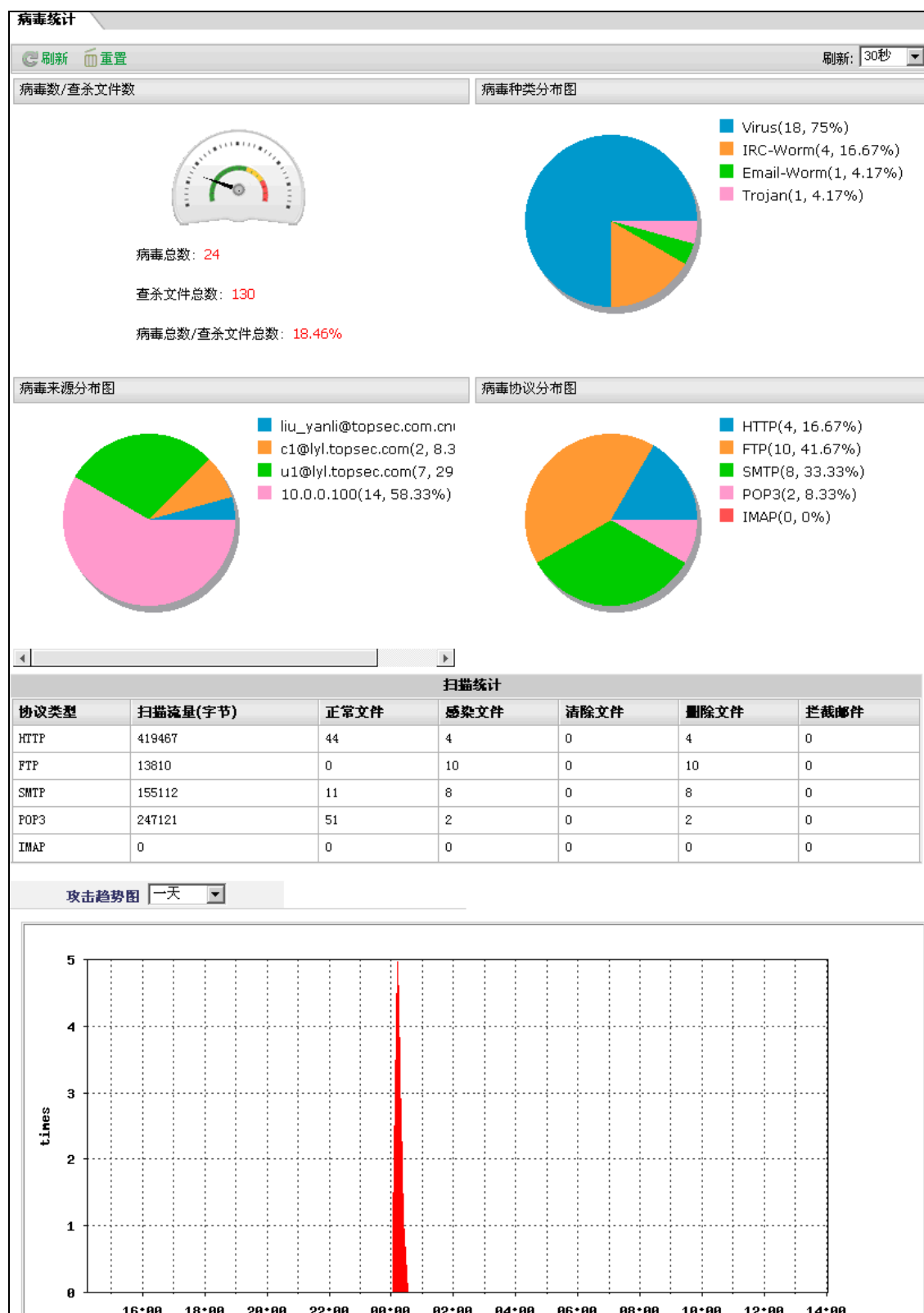
点击页面左上角的“重置”清空统计数据，同时统计开始时间也会被重置。

5.7 病毒统计

病毒统计部分主要提供各种病毒扫描情况的统计信息，包括病毒数/查杀文件数、病毒总类分布图、病毒来源分布图、病毒协议分布图以及扫描各种协议数据的数据流量、正常文件数、感染文件数、清除文件数、删除文件数和拦截文件数目等，另外还会显示出一天/一周/一月的攻击趋势图等。

1) 查看病毒统计

选择 **系统监视** > **病毒统计**，进入“病毒统计”页面，如下图所示。



“攻击趋势图”则给出了一天、一周、一月不同的时间点或时间段内受到攻击数的统计趋势。在“攻击趋势图”右侧的下拉框内可以选择攻击趋势图的统计周期，可选项包括：一天、一周和一月。

2) 刷新病毒统计

在页面右侧“刷新”栏内设定刷新周期，可选项包括：10 秒、30 秒、1 分钟、10 分钟和不刷新；点击“刷新”刷新当前页面。

3) 清空病毒统计

点击页面左上角的“重置”清空统计数据。

5.8 病毒排名

根据系统对病毒、感染病毒主机和病毒来源的统计信息，网络卫士安全网关可以进行病毒排名、感染病毒主机排名以及病毒来源排名，方便管理员掌握网络内的病毒感染情况。

5.8.1 病毒排名

按照病毒攻击次数排名，系统列出了从“开始”时间算起的事件及事件本身的详细内容，包括：病毒名称、危害级别、处理方式、协议、次数、最近发现时间以及病毒来源等信息。

1) 查看病毒排名

选择 **系统监视** > **病毒排名**，选择“病毒排名”页签，进入“病毒排名”页面，如下图所示。

病毒排名						
刷新		重置		总计: 10		
病毒名称	危害级别	处理方式	协议	次数	最近发现时间	病毒来源
Virus.MSWord.Melissa	高	删除	FTP	10	2009.11.26-17:02:14	10.0.0.100
IRC-Worm.Win32.Buffy.b	高	删除	SMTP	4	2009.11.26-17:07:54	ui@lyl.topsec.com
Virus.DOS.Omega.440	高	删除	SMTP	2	2009.11.26-17:10:26	ui@lyl.topsec.com
Virus.DOS.Jerusalem.b	高	删除	SMTP	2	2009.11.27-09:41:06	liu_yanli@topsec.com.cn
Virus.BAT.282	高	删除	HTTP	1	2009.11.26-17:03:03	10.0.0.100
Virus.DOS.Highlander.477	高	删除	POP3	1	2009.11.26-17:06:41	ci@lyl.topsec.com
Email-Worm.VBS.BubbleBoy	高	删除	SMTP	1	2009.11.26-17:07:54	ui@lyl.topsec.com
Trojan.DOS.QHA.h	高	删除	SMTP	1	2009.11.26-17:10:26	ui@lyl.topsec.com
Virus.DOS.Quake.518	高	删除	SMTP	1	2009.11.26-17:10:26	ui@lyl.topsec.com
Virus.BAT.Sailor	高	删除	SMTP	1	2009.11.26-17:10:26	ui@lyl.topsec.com

点击统计信息关键字右侧向上或向下的箭头可以将病毒统计信息按照该关键字进行升序或降序的排名，上图则为按照病毒攻击“次数”进行的升序排名。

点击病毒名称可以查看该病毒的攻击方向及次数，如下图所示。

病毒排名

感染病毒主机排名

病毒来源排名

刷新重置

总计: 10

病毒名称	危害级别	处理方式	协议	次数	最近发现时间	病毒来源
Virus.MSWord.Melissa	主机IP	方向	次数	17	10.0.0.100	
IRC-Worm.Win32.Buffy.b	10.0.0.100	被攻击	1	56	ui@lyl.topsec.com	
Virus.DOS.Omega.440	10.0.0.100	攻击	1	28	ui@lyl.topsec.com	
Virus.DOS.Jerusalem.b	100.0.0.100	攻击	1	09	liu_yanli@topsec.com.cn	
Virus.BAT.282	100.0.0.100	被攻击	1	05	10.0.0.100	
Virus.DOS.Highlander.477				43	ci@lyl.topsec.com	
Email-Worm.VBS.BubbleBoy				56	ui@lyl.topsec.com	
Trojan.DOS.QHA.h				28	ui@lyl.topsec.com	
Virus.DOS.Quake.518				28	ui@lyl.topsec.com	
Virus.BAT.Sailor				28	ui@lyl.topsec.com	

2) 刷新攻击排名

点击页面左上角的“刷新”，界面中显示系统当前的攻击排名及其详细信息。

3) 清空攻击排名

点击页面左上角的“重置”清空统计数据。

5.8.2 感染病毒主机排名

1) 查看感染病毒主机排名

选择 **系统监视** > **病毒排名**，选择“感染病毒主机排名”页签，进入“感染病毒主机排名”页面，如下图所示。

病毒排名		感染病毒主机排名		病毒来源排名	
刷新 重置				总计: 3	
主机IP	低风险	一般风险	高风险		
10.0.0.100	0	0	24		
192.168.1.169	0	0	1		
100.0.0.100	0	0	23		

点击统计信息关键字右侧向上或向下的箭头可以将病感染病毒主机按照该关键字进行升序或降序排名，上图则为按照“低风险”进行的升序排名。

点击主机 IP 可以查看该主机感染病毒的详细信息，如下图所示。

病毒排名

感染病毒主机排名

病毒来源排名

刷新

重置

总计: 3

主机IP

10.0.0.100

192.168.1.169

100.0.0.100

低风险

一般风险

高风险

病毒名称	方向	危害级别	次数
Virus.MSWord.Melissa	攻击	高	10
IRC-Worm.Win32.Buffy.b	攻击	高	4
Virus.DOS.Jerusalem.b	攻击	高	2
Virus.BAT.282	攻击	高	1
Virus.DOS.Highlander.477	被攻击	高	1
Virus.DOS.Omega.440	被攻击	高	1
Email-Worm.VBS.BubbleBoy	攻击	高	1
Virus.DOS.Omega.440	攻击	高	1
Trojan.DOS.QHA.h	攻击	高	1
Virus.DOS.Quake.518	攻击	高	1
Virus.BAT.Sailor	攻击	高	1

24

1

23

2) 刷新感染病毒主机排名

点击页面左上角的“刷新”，界面中显示系统当前的感染病毒主机排名。

3) 清空感染病毒主机排名

点击页面左上角的“重置”清空统计数据。

5.8.3 病毒来源排名

1) 查看病毒来源排名

选择 **系统监视 > 病毒排名**，选择“病毒来源排名”页签，进入“病毒来源排名”页面，如下图所示。

病毒排名	感染病毒主机排名	病毒来源排名
刷新 重置 总计: 4		
病毒来源 10.0.0.100 ul@lzl.topsec.com cl@lzl.topsec.com liu_yanli@topsec.com.cn		
次数 14 7 2 1		
最近发现时间 2009.11.26-17:03:20 2009.11.27-09:40:44 2009.11.26-17:06:43 2009.11.27-09:41:09		

点击统计信息关键字右侧向上或向下的箭头可以将病毒来源按照该关键字进行升序或降序的排名，上图则为按照病毒攻击“次数”进行的降序排列。

2) 刷新感染病毒主机排名

点击页面左上角的“刷新”，界面中显示系统当前的感染病毒主机排名。

3) 清空感染病毒主机排名

点击页面左上角的“重置”清空统计数据。

6 网络管理

网络卫士安全网关作为一种网关型产品，通常部署在各个安全区域的入口或交点，可以通过交换机或 HUB 将安全区收缩为一个入口，并将此入口点连接到安全网关的网络接口。因此在安装网络卫士安全网关之前，网络管理人员应根据网络应用的实际情况以及网络中主机、服务器等设备的安全属性来规划安全区域。

本章主要包括：

- 网络规划：主要介绍如何根据企业的实际网络情况进行网络规划。
- 接口设置：主要介绍如何设置网络卫士安全网关上的物理接口、子接口以及端口聚合，包括接口属性和 IP 地址设置等。
- 二层网络：主要介绍如何在网络卫士安全网关上设置 VLAN、ARP 和 MAC 地址表等信息。
- 路由：介绍网络卫士安全网关支持的路由协议，及各种路由的设置方式。
- 接入：主要介绍如何设置 ADSL 连接、虚拟转发线路、聚合链路、VLAN-VPN 的相关参数。
- DHCP：主要介绍如何将网络卫士安全网关作为 DHCP 服务器、DHCP 客户端和 DHCP 中继使用。
- 流量管理：主要介绍网络卫士安全网关的带宽管理功能，主要包括 QoS 对象设置、各种流量统计以及连接统计设置。
- IP 探测：主要介绍 IP 探测参数设置。
- 域名解析：主要介绍如何在网络卫士安全网关上设置 DNS 服务器。

6.1 网络规划

在网络规划时，一般会碰到两种情况：

1) 在当前运行的网络中添加网络卫士安全网关。

这种情况下，网络卫士安全网关的安装环境为一个已经建立并正在运行的网络，目的通常是增强现有网络的防御能力。在此类网络中部署安全网关，往往要求尽可能少地改动或禁止改动网络节点的网络属性，如网络拓扑结构、网络设备地址等，并要求安全网关的接入对网络通信造成的影响最少，尽可能地做到安全网关部署透明。

这种环境下，部署的网络卫士安全网关最好采用透明模式或者虚拟线方式。在透明模式下，如果在同一 VLAN 中转发数据报文，网络卫士安全网关将不改变通信数据包的包头信息，这样可以避免各个防火区域中应用设备的物理地址的刷新。同时，网络卫士安全网关可以在设置了接口 IP 的不同 VLAN 之间路由转发数据报文。在虚拟线模式下，将安

全网关的 2 个物理接口加入一个虚拟线组后，从一个接口接收包时，除了目的地址是安全网关地址的数据报文外，会直接从另一个接口转发出去，不经过二层交换以及三层路由的检查过程。

2) 在设计网络结构和部署网络设备的初始阶段，充分考虑了网络的安全问题，并已将网络卫士安全网关的安全和通信等功能融入网络设计方案。

在这种情形下，通常可以启用安全网关的通信功能，如路由、地址转换等。最佳的工作模式为混合模式，即同时使用安全网关的透明功能和路由功能。透明模式支持把同一网段的网络区域划分为不同的防火区，主要适用于基于业务的 IP 分配方案，可以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。路由模式支持将路由信息转发到其它防火区，减少安全网关应用带来的网络管理的工作量。网络卫士安全网关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完全可以代替内网路由器。该工作模式下，网络卫士安全网关可以友好地支持网络扩展，如可以对安全网关原有的配置不作改变或少量修改，实现在原有网络基础上增加网段或主机的功能。

网络规划实例

下面以一个网络卫士安全网关部署案例说明网络的划分：

方案中设计了 4 个防火区，分别是：

- 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

其中内部网络防火区包括两个子网：安全子网 A 和安全子网 B；LAN-1 跨两个防火区：公共网络防火区和安全服务防火区。

安全区与安全网关接口的对应关系如下：

- 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

下图为规划好的网络拓扑图。

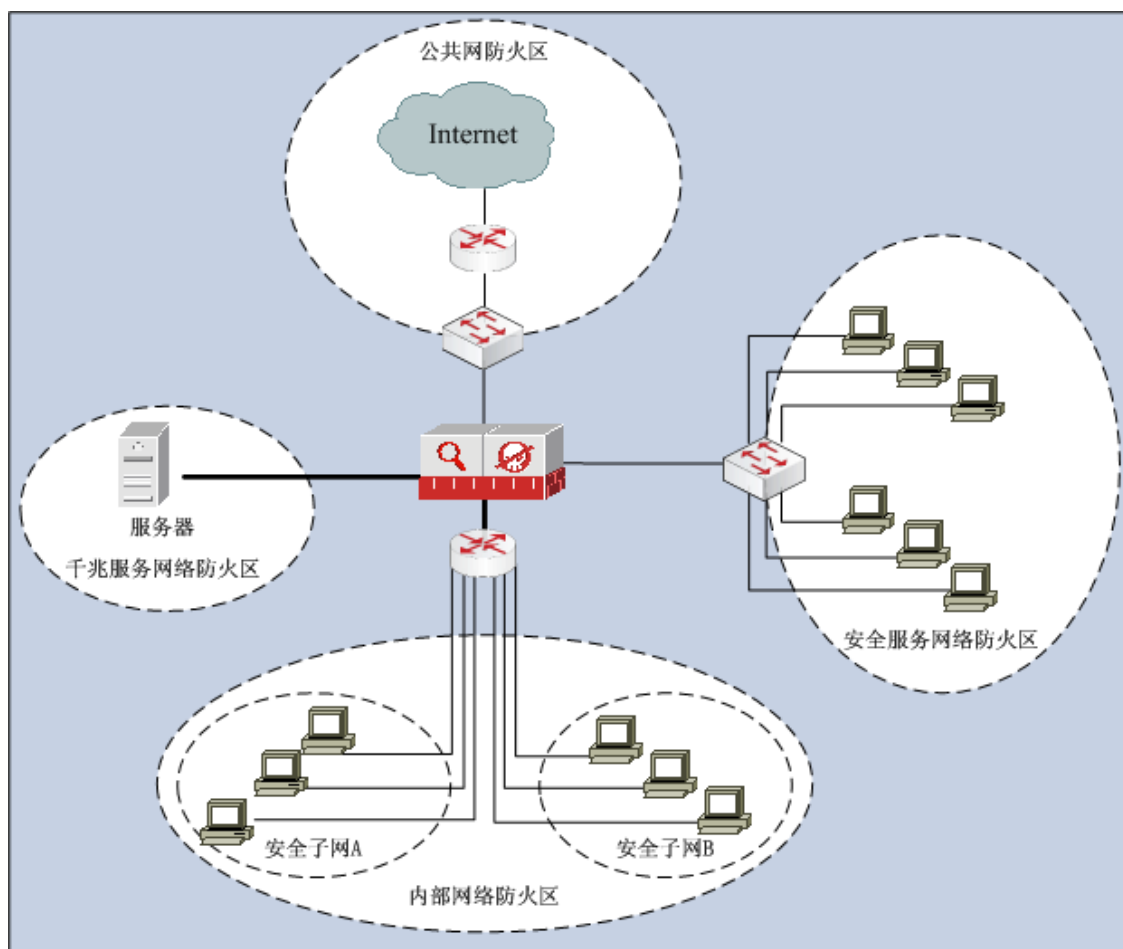


图 6-1 网络卫士安全网关部署案例示意图

6.2 接口设置

接口是网络卫士安全网关与网络中其他设备交换数据并相互作用的部分，网络卫士安全网关的接口分为物理接口和逻辑接口。

物理接口是指真实存在，并且有对应硬件器件支持的接口，如设备上的 eth0、eth1、eth2 和 eth3 等，即以太网接口，广义的物理接口还包括 Console 口、AUX 接口等，此处所指的接口仅是以太网接口，网络卫士安全网关通过它与其他网络设备交换数据。

逻辑接口是指能够实现数据交换功能但物理上不存在，并且需要通过配置建立的接口，包括子接口、虚接口和聚合接口。

a) 子接口提供了在一个物理接口上支持多个逻辑接口或网络互连的功能，即将多个逻辑接口与一个物理接口建立关联，在这些逻辑接口工作时，共用物理接口的物理参数配置，但有各自的链路层和网络层配置参数。

b) 虚接口是用于配置一个虚拟访问的接口，如在使用 VPN、ADSL 等功能时，需要创建一个虚拟访问接口用于和对端交换数据，虚接口在链路断开后自动删除。

c) TOS 支持将多个端口聚合成一个逻辑端口。端口聚合可以使设备之间的带宽成倍增加、增强端口灵活性并提供链路冗余。当聚合端口内的某条链路出现故障时，该链路的流量将自动转移到其余链路上。

本节主要介绍物理接口以及逻辑接口中子接口和聚合端口的配置方法，关于 IPsec 虚拟接口的配置方法请参见《TopGate 管理手册——IPsec VPN 配置》。

6.2.1 物理接口

网络卫士安全网关根据设备型号的不同支持快速以太网接口（速率为 10/100Mbit/s）和千兆以太网接口（速率为 1000Mbit/s），在进行接口配置时，协商及速度等属性一般为系统自动匹配模式，MTU 及 MSS 也采用系统默认值，一般不需要用户配置，但是根据用户需要，当接口采用 GE（千兆以太网）电接口时（同时支持 10/100/1000Mbit/s），也可以由用户强制指定接口速度。此外，采用不同的链路层封装格式，其缺省的 MTU 值也不同。

说明

- ✧ 对于 TOPSEC8.8 平台的产品，设备面板上扩展卡位的标识名称为 Eth1、Eth2、Eth3 等。扩展模块上的接口则以 0、1、2、3……的形式标识。安装模块后，TOS 系统识别各接口的名称为：扩展卡位标识+扩展模块的接口标识，例如 Eth1 卡位的接口 2 会被识别为 Eth12，其他接口以此类推。
- ✧ 对于 Topsec6.5 平台的产品，设备面板上扩展卡位的标识名称为 Slot1，扩展模块上的接口则以 0、1、2、3……的形式标识。安装模块后，TOS 系统识别各接口的名称为：扩展卡位标识+扩展模块的接口标识，例如 Slot1 卡位的接口 2 会被识别为 Eth12，其他接口以此类推。

对网络卫士安全网关的物理接口的属性进行设置，具体步骤如下：

1) 在管理界面左侧导航菜单中选择 **网络管理 > 接口**，或在 WEBUI 界面右上方的菜单栏选择 **接口配置**，选择“物理接口”页签，可以看到安全网关的所有物理接口的相关属性，如下图所示。

物理接口		子接口							
接口名称	描述	接口模式	地址	MTU	状态	链接	协商	速率	设置
eth0	intranet	路由	192.168.83.233/255.255.255.0	1500	启用		半双工	10M	
eth1	internet	路由	10.1.1.1/255.255.255.0	1500	启用				
eth2	ssn	交换trunk(3, 102)		1500	启用				
eth3		交换trunk(3, 103)		1500	启用				

2) 点击该接口对应的设置图标，可以设置接口的属性及相关参数，如下图所示。

接口设置			
名称	eth0 (00:13:32:02:2C:44)		
描述	intranet		
状态	☐ 停用		
模式	☒ 路由 ☐ 交换		
地址	掩码	非同步地址	
		☐	添加
地址	掩码	属性	删除
192.168.83.233	255.255.255.0		
确定 取消			

a) 设置接口的基本属性：包括接口工作在路由模式还是交换模式、是否启用该接口以及接口描述信息。

参数	说明
名称	显示接口名称及其 MAC 地址。
描述	用户可以输入对该接口的简要描述。
状态	默认接口为“启用”状态，表示可以使用该接口；如勾选“停用”，则表示该接口将不会工作，该接口所在的区域将无法和其他接口进行通讯。
模式	设定接口工作在路由模式、交换模式或 IDS 监听模式。 当接口工作在 IDS 监听模式时，接口对于接收的数据报文只作检测及报警，不作转发。

b) 设置接口在不同工作模式下的属性。

路由模式基本属性设置

当在“基本信息”处设置接口工作在“路由”模式时，需要设置接口的 IP 地址及其掩码，如下图所示。

路由模式			
地址	掩码	非同步地址	
		☐	添加
地址	掩码	属性	删除
192.168.83.237	255.255.255.0		

上图的参数说明见下表所示：

参数	说明
地址/掩码	输入接口的 IP 地址及其子网掩码。 说明： 1) 可以为路由接口设置多个 IP 地址。

参数	说明
	2) 网络卫士安全网关不支持不同的物理接口配置相同的 IP 地址或 IP 地址在同一子网内。 3) 如果在某接口启动了 DHCP 客户端进程, 则不能手动添加该接口的 IP 地址。
非同步地址	如果在网络中配置了双机热备功能, 则设置心跳口 IP 时必须要选择“非同步地址”, 否则接口的 IP 地址信息会在主/从设备同步运行状态时被对方覆盖。对于双机热备中设置为“从属机”身份的安全网关, 其管理 IP 必须选择“非同步地址”, 否则无法对从属机进行管理。关于双机热备的配置请参见 16.2 高可用性。
添加	如果“地址/掩码”设置正确, 点击“添加”按钮, 则新添加接口的 IP 地址会显示在列表中。
删除	点击 IP 地址对应的删除图标, 可以删除添加的 IP 地址。 说明: 如果在某接口启动了 DHCP 服务器进程, 则不能删除该接口的 IP 地址。

交换模式基本属性设置

当在“基本信息”处设置接口工作在“交换”模式时, 需要设置接口类型为“access”或“trunk”的接口, 及其所属 VLAN 的 ID 号。

① 当交换接口为“access”口时, 界面如下图所示。

交换模式

类型 ☒ access ☐ trunk

Access [1 - 4094]

② 当交换接口为“trunk”接口时, 则表示该交换接口可以属于多个 VLAN, 界面如下图所示。

交换模式

类型 ☐ access ☒ trunk

VLAN范围 [1 - 4094, 多个范围中间用逗号分隔]

封装类型 ☒ 802.1Q ☐ ISL

参数说明见下表所示:

参数	说明
类型	设置该交换接口的类型。可选值为 access 和 trunk。
Access	仅当“类型”为“access”时, 需要设置该项。“access”交换接口只属于一个 VLAN, 此参数用于指定 Access 口所属的 VLAN ID 号码。
VLAN 范围	仅当“类型”为“Trunk”时, 需要设置该项。 用于设置该 Trunk 接口属于哪些 VLAN。VLAN 值的范围为 1-4094。 格式举例: 1-10 表示属于 VLAN1 到 VLAN 10; 1, 10 表示属于 VLAN1 和 VLAN10。

参数	说明
封装类型	仅当“类型”为“Trunk”时，需要设置该项。 用于设置 Trunk 接口数据的封装方式，系统支持两种数据封装方式：802.1Q(标准 IEEE802.1Q 协议)方式和 ISL 方式。

3) 设置完成后，点击“确定”按钮完成接口属性设置。

4) 查看接口相关设置。

在 WUBUI 界面点击具体的“接口名称”，可以查看该接口的流量统计信息，如下图所示。

物理接口		子接口							
接口名称	描述	接口模式	地址	MTU	状态	链接	协商	速率	设置
eth0	intranet	路由	192.168.83.233/255.255.255.0	1500	启用		半双工	10M	
eth1	internet	路由	10.1.1.1/255.255.255.0	1500	启用				
eth2	ssn	交换tr							
eth3		交换tr							

统计内容	统计值
interface eth0 receive packets	6168065
receive bytes	356740874
tcp receive packets	134956
tcp receive bytes	15257142
udp receive packets	704056
udp receive bytes	60179696
icmp receive packets	155643
icmp receive bytes	11512787
transmit packets	808876
transmit bytes	87906884
input rate	2358 bps
output rate	358 bps

6.2.2 子接口

子接口是在路由模式的单个物理接口或者聚合端口（请参见 [6.5.3链路聚合](#)）上配置的多个逻辑接口，所有的子接口共用物理接口的物理参数配置，但有各自的链路层和网络层配置参数，子接口提供了在一个物理接口或聚合端口上支持多个网络互连的功能，为用户提供提供了很高的灵活性。

说明

◇ 当物理接口工作在交换模式和 IDS 监听模式时，不能添加子接口。

设置子接口的具体步骤如下：

1) 在管理界面左侧导航菜单中选择 **网络管理 > 接口**，或在WEBUI界面右上方的菜单栏选择 **接口配置**，然后选择“子接口”页签，进入子接口配置界面，如下图所示。

物理接口

子接口

+ 添加子接口

名称	描述	地址	MTU	状态	操作

2) 添加子接口。

a) 点击“添加子接口”，进入子接口添加界面，如下图所示。

添加子接口

路由接口 -选择接口-

添加单个子接口 ☒ [0-31]

添加子接口范围 ☐ -

确定
取消

界面中各参数的说明如下：

参数	说明
路由接口	选择要在其下添加子接口的物理接口或聚合端口，该接口必须为路由接口。
添加单个子接口	添加单个子接口的 ID 号，范围为 0-31。添加后，子接口的名称为“v+路由接口名称.子接口 ID 号”，如 veth0.01,veth1.02 或 vbond0.01。
添加子接口范围	添加多个子接口的 ID 号，可以一次在某个物理接口下添加多个子接口。范围为 0-31。

b) 点击“确定”完成子接口添加。

添加完成后界面如下图所示，可以看出，子接口默认为“停用”状态。

物理接口

子接口

+ 添加子接口

名称	描述	地址	MTU	状态	操作
veth0.01			1500	停用	 

c) 删除子接口

点击“操作”栏中的删除图标可以删除该子接口。

3) 设置子接口的属性。

在已经添加的子接口后，点击“操作”一栏的编辑图标，进入设定接口属性界面，如下图所示。

子接口设置

名称 veth0.05

描述

状态 ☒ 停用

接口地址

地址

掩码

非同步地址 ☐

添加

地址

掩码

属性

删除

VLAN-ID [0-4094]

确定
取消

接口参数说明如下：

参数	说明
描述	用户可以输入对该子接口的简要描述。
状态	设置该子接口是否可用；默认接口为“启用”状态，表示可以使用该子接口；如勾选“停用”，则表示该子接口将不会工作，该子接口状态将会显示为“停用”。 说明： 当物理接口为“禁用”状态时，不允许启用属于它的子接口。
地址/掩码	输入子接口的 IP 地址及其子网掩码。 说明： 1) 可以为子接口设置多个 IP 地址。 2) 不同的物理接口和子接口不能配置相同的 IP 地址，也不能配置同一子网内的不同的 IP 地址。 3) 如果在某接口启动了 DHCP 客户端进程，则不能手动添加该接口的 IP 地址。
非同步地址	如果在网络中配置了双机热备功能，则设置心跳口IP时必须要选择“非同步地址”，否则接口的IP地址信息会在主/从设备同步运行状态时被对方覆盖。对于双机热备中设置为“从属机”身份的安全网关，其管理IP必须选择“非同步地址”，否则无法对从属机进行管理。关于双机热备的配置请参见16.2 高可用性。
添加	如果“地址/掩码”设置正确，点击“添加”按钮，则新添加接口的 IP 地址会显示在列表中。
删除	点击 IP 地址对应的删除图标，可以删除添加的 IP 地址。 说明： 如果在子接口上启动了 DHCP 服务器进程，则不能删除该子接口的 IP 地址。
VLAN-ID	表示该子接口所属的 VLAN ID 号，默认为 0。只有当安全网关的物理接口需要与交换机的 Trunk 口连接时需要设置该项，此时每个子接口必须设置不同的 VLAN ID 号。 说明： 当子接口接收的报文带有 802.1q 封装时，解析报文的 802.1q 封装信息，如果封装标签与子接口的 dot1q-vid 值一致，去掉报文的 802.1q 封装头继续转发，否则丢弃报文。 当子接口发送报文时，如果子接口的 dot1q-vid 配置不为 0，先对报文做

参数	说明
	802.1q 封装，然后再发送出去。

点击“确定”，完成子接口属性的设定。

4) 查看子接口的流量统计信息。

在 WUBUI 界面上点击子接口的“名称”，可以查看该子接口的各个协议的流量统计信息。

6.3 二层网络

主要介绍如何在网络卫士安全网关上设置 VLAN、ARP 和 MAC 地址表等信息。

6.3.1 ARP

ARP 即地址解析协议，主要用于从 IP 地址到以太网 MAC 地址的解析。ARP 表用于存储 IP 地址到 MAC 地址的映射，其内容包括设备动态学习到的动态 ARP 表项，和管理员手工添加的静态 ARP 表项两种。其中，动态 ARP 表项是动态更新的，缓存项经过一定的时间将被删除；静态 ARP 表项则不存在老化问题，而且能够有效地防止 ARP 欺骗。

管理员可以手工添加静态 ARP 条目、删除 ARP 条目，或者一次清空 ARP 表，具体操作步骤如下：

1) 在左侧导航菜单中选择 **网络管理 > 二层网络**，点击“ARP”页签，如下图所示。

ARP				
VLAN				
MAC				
+ 添加		🗑 清空		总计: 3
IP地址	MAC地址	状态	接口	删除
192.168.83.225	00:11:d8:a8:9c:4e	正常	eth0	
192.168.83.224	00:50:04:c3:b0:31	正常	eth0	
192.168.83.220	00:0d:61:9f:bd:26	正常	eth0	

2) 添加静态 ARP 表项。

点击“添加”，如下图。

添加配置	
选择接口	eth0
IP地址	*
物理地址	* [格式如 AA:BB:CC:DD:EE:FF]
确定 取消	

参数说明如下表所示：

参数	说明
选择接口	设置源地址所在区域所对应的安全网关设备路由接口或 VLAN 虚接口名称。
IP 地址	输入 IP 地址格式字符串。
物理地址	输入 IP 地址对应的 MAC 地址。

点击“确定”按钮，在 ARP 表中新添加状态为“静态”的 ARP 表项，如下图所示。

ARP VLAN MAC				
+ 添加 清空		总计: 6		
IP地址	MAC地址	状态	接口	删除
192.168.83.225	00:11:d8:a8:9c:4e	正常	eth0	
192.168.83.227	00:0d:67:78:86:34	静态	eth0	
192.168.83.40	00:16:d3:23:46:76	正常	eth0	
192.168.83.224	00:50:04:e3:b0:31	正常	eth0	
192.168.83.220	00:0d:61:9f:bd:26	正常	eth0	
192.168.83.226	00:11:d8:68:00:80	正常	eth0	

3) 删除 ARP 条目

点击某条目对应的删除图标，可以删除该条 ARP 条目。

4) 清空 ARP 表项。

点击“清空”，则下面 ARP 表中的所有内容将会一次删除。

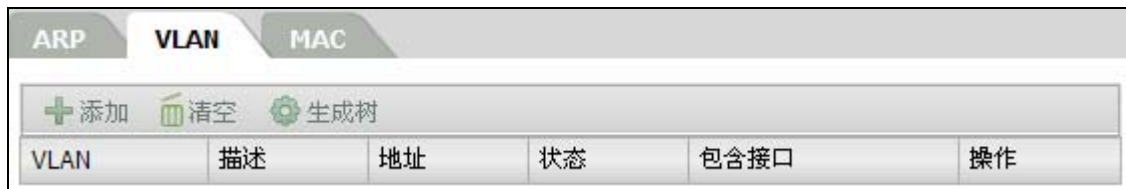
6.3.2 VLAN

当物理接口工作在交换模式下时，网络卫士安全网关可以很好地支持 VLAN。交换接口的工作模式包括 access 和 trunk 模式，“access”模式表示该交换接口只属于一个 VLAN，“trunk”模式表示该交换接口可以属于多个 VLAN。

6.3.2.1 添加 VLAN 到安全网关设备

添加 VLAN 的具体操作步骤如下：

- 1) 在左侧导航菜单中选择 **网络管理** > **二层网络**，点击“VLAN”页签，如下图所示。



- 2) 添加 VLAN

- a) 点击“添加”，可以一次添加一个或多个 VLAN。界面如下图所示。

添加配置

添加单个VLAN ☒ [1-4094]

添加VLAN范围 ☐ - [总数最多是1024个]

- b) 设置参数。

界面中各参数的说明如下：

参数	说明
添加单个 VLAN	添加单个 VLAN 的 ID 号，范围为 1-4094。添加后，子接口的名称为“vlan.ID 号”，如 vlan.001。
添加 VLAN 范围	添加多个 VLAN 的 ID 号，可以一次添加多个 VLAN。范围为 1-4094。 说明： 起始 VLAN ID 和终止 VLAN ID 中设置的数值既可以相同也可以不同，但起始 VLAN ID 一定不能大于终止 VLAN ID。数值不同时，表示添加的是一段 ID 连续的 VLAN；数值相同时，表示添加的是某一个 VLAN。

- c) 设置完成后，点击“确定”按钮，如果添加 VLAN 成功，则新添加的 VLAN 会显示在界面中。放弃添加点击“取消”返回上一界面。

- 3) 加入交换接口到 VLAN，

添加VLAN到安全网关设备后，再选择相应的工作在交换模式的物理接口加入到已添加的VLAN中。物理接口类型可以设置为access模式，即只属于一个VLAN。也可以设置

为trunk模式，即同时属于多个VLAN。网络卫士安全网关支持 802.1Q及ISL VLAN协议。
具体请参见[6.2.1物理接口](#)。

4) 删除 VLAN

点击某个 VLAN 后“操作”一栏对应的“删除”图标可以删除该 VLAN。

点击“清空”则会一次性删除所有的 VLAN 设置信息。

6.3.2.2 设定 VLAN 虚接口的属性

添加 VLAN 后，需要给 VLAN 虚接口配置接口 IP 地址和子网掩码等属性。具体方法为：

1) 若要设置 VLAN 虚接口的属性，可以点击“操作”一栏对应的修改图标进行修改。界面如下图所示：

VLAN设置

名称: vlan.0001

描述:

状态: ☐ 停用

接口地址

地址: 掩码: 非同步地址: ☐

地址	掩码	属性	删除
▼ 高级 虚系统ID: 0 [0-254] 确定 取消			

VLAN 虚接口的属性参数说明如下：

参数	说明
描述	用户可以输入对该接口的简要描述。
状态	默认接口为“启用”状态，表示可以使用该 VLAN；如果勾选“停用”，则表示该 VLAN 将不会工作，该 VLAN 所在的区域将无法和其他接口进行通讯。
地址/掩码	输入该 VLAN 虚接口的 IP 地址及其子网掩码。 说明： 网络卫士安全网关不支持不同的 VLAN 虚接口之间、及与路由接口之间配置相同的 IP 地址或 IP 地址在同一子网内。
非同步地址	当设备为“双机热备”部署时才需要勾选该选项。 说明： 1) 如果不勾选该项，该 VLAN 虚接口的 IP 地址在主/从设备同步运行状

参数	说明
	态时会被对方的 IP 地址所覆盖。 2) 对于双机热备中设置为“从属机”身份的安全网关，其管理IP必须选择“非同步地址”，否则无法对从属机进行管理。关于双机热备的配置请参见 16.2高可用性 。
添加	点击“添加”按钮，如果设置正确，则新添加接口的 IP 地址会显示在列表中。
虚系统 ID	该接口所属的虚系统 ID 号，范围为 0-254，默认为 0，表示不属于任何虚系统。

点击“确定”按钮完成 VLAN 虚接口的属性设置。

2) 对于已经添加的接口 IP 地址，无法修改其参数，只能点击删除图标进行删除。

6.3.2.3 生成树属性设置

交换接口的生成树功能在缺省情况下处于关闭状态。如果网络中需要通过环路设计来提供网络的冗余容错能力，而同时又需要防止产生环路，则需要开启生成树。当用户可以确认该交换接口连接的部分不存在环路时，也可以关闭已经打开的生成树功能。网络卫士安全网关支持的生成树协议为 CISCO 公司的 PVST，即每个 VLAN 维护一个生成树。

管理员需要首先启用生成树协议，然后才能设置生成树协议的参数。

生成树属性设置步骤如下：

1) 在左侧导航菜单中选择 **网络管理 > 二层网络**，点击“VLAN”页签，如下图所示。

ARP

VLAN

MAC

+

添加

🗑️

清空

⚙️

生成树

VLAN	描述	地址	状态	包含接口	操作
vlan.0001			启用		✎ 🔄
vlan.0002			启用		✎ 🔄
vlan.0003			启用		✎ 🔄
vlan.0004			启用		✎ 🔄
vlan.0005			启用		✎ 🔄

2) 开启 PVST 生成树模式。

生成树协议默认为“关闭”状态。点击“生成树”按钮，进入生成树协议设置界面，如下图所示。

生成树

☐ 开启 (缺省为PVST模式)

应用
返回

勾选“开启”后，点击“应用”即可开启 PVST 生成树模式，表示每个 VLAN 维护一个生成树。

ARP

VLAN

MAC

+

添加

🗑️

清空

⚙️

生成树

VLAN	描述	地址	状态	包含接口	生成树	操作
vlan.0001			启用			 
vlan.0002			启用			 
vlan.0003			启用			 
vlan.0004			启用			 
vlan.0005			启用			 

3) 配制生成树协议的参数

“PVST”：表示每个 VLAN 维护一个生成树，需要点击每个 VLAN 后显示的生成树图标“”为其配置生成树参数。

a) 点击生成树图标“”，进入如下图界面。

生成树设定

VLAN ID 0001

生成树状态 打开 ☐ 关闭 ☒

优先级 * [1-65535]

HELLO TIME * [1-65535]

FORWARD DELAY * [1-65535]

MAX AGE * [1-65535]

确定
恢复默认
设为根桥
取消

各参数的具体说明如下：

参数	说明
生成树状态	PVST 模式下，可以设置当前 VLAN 是否开启生成树。
优先级	设置网桥的优先级，数值越小优先级越高。 默认值为 32768，范围为 1~65535。

参数	说明
HELLO TIME	BPDU 发送时间间隔。单位：秒。 默认设置为 2 秒，范围为 1~65535。 注意：呼叫时间不能大于网桥的最大老化时间（Max Age）。否则，将出现错误信息。
FORWARD DELAY	BPDU 转发延迟时间间隔，是指交换机的端口从阻塞状态转为转发状态所用的监听时间。单位：秒。 默认设置为 15 秒，范围为 1~65535。
MAX AGE	最大老化时间，BPDU(网桥协议数据单元)的最大老化时间。单位：秒。 默认设置为 20 秒，范围为 1~65535。

b) 设置完成各参数后，点击“确定”按钮完成操作。在“生成树状态”下方可以查看生成树的状态。

点击“恢复默认”则上述所有参数恢复系统默认值。

点击“设为根桥”则将网络卫士安全网关设定为生成树的根桥。

点击“取消”则返回 VLAN 设置页面，界面参数修改无效。

6.3.3 MAC

当网络卫士安全网关的接口工作在交换模式时，根据 MAC 地址表来对报文进行转发。MAC 地址表的表项包含 MAC 地址、转发的物理接口号以及 VLAN 虚接口号。

MAC 地址表中的表项包括静态表项和动态表项两种：

➤ 动态表项

交换接口根据收到数据帧中的源 MAC 地址建立该地址同端口的映射，并将其写入 MAC 地址表中，生成动态 MAC 表项。动态表项动态更新，无需管理员配置。

➤ 静态表项

静态表项是由管理员配置，不会随着时间而老化。

设备在转发报文时，将首先查询 MAC 地址表项中是否包含与目的 MAC 地址匹配的表项。如果有匹配的表项时，则将报文通过相应的端口进行转发。如果没有相应的匹配项，则采取广播方式向除接收端口外的所有端口转发该数据帧。

MAC 表配置的具体操作步骤如下：

1) 在左侧导航菜单中选择 **网络管理 > 二层网络**，点击“MAC”页签，可以查看到所有静态和动态 MAC 表项，如下图所示。

ARP	VLAN	MAC		
+ 添加静态项 清除静态项 总计: 0				
MAC地址	Vlan	接口	静态	删除

上图中，“静态”一栏如果显示为 1，表示该表项为静态 MAC 表项；如果显示为 0，表示该接口为动态学习到的 MAC 表项。

2) 添加静态项

a) 点击“添加静态项”，进行静态 MAC 表项的添加，如下图所示。

各参数的具体说明如下：

参数	说明
VLAN	选择通过哪个 VLAN 虚拟接口进行转发。 说明： 当“选择端口”处设定的交换接口工作在“access”模式时，必须选择其所属的 VLAN 的 ID 号；当“选择端口”处设定的交换接口工作在“Trunk”模式时，可以选择 VLAN 范围中的一个 ID 号。
接口	选择转发的物理接口。只能选择工作在交换模式的物理接口名。
物理地址	输入匹配的 MAC 地址。

b) 设置完成后，点击“确定”按钮，点击“取消”则放弃添加，返回上一界面。

3) 删除静态 MAC 条目

点击某条目所在行的删除图标，可以删除该表项。

点击“清除静态项”则一次性删除所有的静态 MAC 地址表项。管理员无法删除动态 MAC 表项。

6.4 路由

网络卫士安全网关可以作为网络中的路由设备使用，支持普通数据报文的转发，管理员可以手工配置静态路由和策略路由，同时支持通过 RIP、OSPF 和 BGP 动态路由协议动态发现路由。其中，策略路由的优先级最高；静态路由和动态发现的路由则在静态路由表中统一管理，通过将各路由协议（包括静态路由）赋予不同的“度量值”，当针对同一目

的地存在不同下一跳的若干条路由时，具有较高“度量值”的路由协议发现的路由将成为当前路由。

对于静态路由和策略路由，网络卫士安全网关支持路由的负载均衡功能，即允许配置多条到同一目的地而且“度量值”相同的路由，此时根据路由的“权重值”选择下一跳；当多条路由的度量值及权重值均相同时，采取轮询方式选择下一跳，从而实现路由的负载均衡。

网络卫士安全网关可以通过定义多播路由，允许 IP 多点广播数据报文穿越网络卫士安全网关。

6.4.1 路由表

网络卫士安全网关转发数据报文的关键是路由表，表中每条路由项都指明分组到某子网或某主机应通过安全网关的哪个物理端口发送，然后就可到达该路径的下一个路由器，或者不再经过别的路由器而传送到直接相连的网络中的目的主机。

当静态路由表中，对于同一目的地存在多条静态路由时，“度量值”小的路由将成为当前的最优路由。“度量值”也相同时，会根据“权重值”做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。

路由表配置步骤如下：

1) 在左侧导航菜单中选择 **网络管理 > 路由**，点击“路由表”页签，可以看到安全网关的路由表，如下图所示。

路由表										
策略路由		动态路由由OSPF		动态路由由RIP		动态路由由BGP		多播路由		
标记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D-Dhcp, I-Ipsec, i-Interface specified										
+ 添加		🗑 清空								总计: 4
目的		网关	标记	度量值	权重值	出接口(属性)		探测ID	删除	
192.168.83.233/32		0.0.0.0	ULi	1	1	lo		-	-	
10.10.10.1/32		0.0.0.0	ULi	1	1	lo		-	-	
192.168.83.0/24		0.0.0.0	UCi	10	1	eth0		-	-	
10.10.10.0/24		0.0.0.0	UCi	200	1	sslvpn0		-	-	

2) 查看路由表

路由表项包括三类：

①静态路由：

由管理员手工配置，“标记”列包含“S”标记；如果添加时指定了“出接口”，还包含“i”标记；如果添加时指定了“网关”，还包含“G”标记；“标记”一栏不显示“U”时，表示该条路由不可用。

②由动态路由协议发现的路由：

需要管理员配置相关的动态路由协议的参数，配置正确时学习到的静态路由将显示在列表中；标记列包含“O”时，表示由 OSPF 协议学习得到；包含“R”表示由 RIP 协议学习得到；包含“B”表示由 BGP 协议学习得到。

③直连路由：

在物理接口或虚接口启用后自动添加在路由表中，包括物理接口和 VLAN 虚接口的直连路由、IPSEC VPN 模块启动后自动添加的静态路由、SSLVPN 模块启动了“全网接入”功能后添加的静态路由、ADSL 拨号成功后自动添加的静态路由。“标记”列包含“C”标记。

3) 添加静态路由

a) 点击“添加”，进入静态路由的添加页面，如下图所示。

The screenshot shows a web-based configuration window titled "添加配置" (Add Configuration). It contains the following fields and controls:

- 目的地址** (Destination Address): Text input field with a red asterisk indicating it is required.
- 目的掩码** (Destination Mask): Text input field with a red asterisk indicating it is required.
- 网关** (Gateway): Text input field.
- 接口** (Interface): Dropdown menu with the placeholder text "-选择接口-" (Select Interface).
- 高级** (Advanced): A collapsed section indicated by a blue downward arrow.
- 度量值** (Metric): Text input field with a range constraint "[1-65535]" to its right.
- 权重值** (Weight): Text input field with a range constraint "[1-128]" to its right.
- 探测ID** (Probe ID): Dropdown menu with the placeholder text "-选择ID-" (Select ID).
- Buttons**: Two buttons at the bottom, "确定" (Confirm) and "取消" (Cancel).

各参数的具体说明请参见下表。

参数	说明
目的地址	用来标识 IP 包的目的地地址或目的网络。需要填写目的地地址转换后的真实地址。 说明： 当目的 IP 地址和掩码均为 0.0.0.0 时，配置的为设备的缺省路由，即当查找路由表失败后，根据缺省路由进行包的转发。
目的掩码	目的 IP 地址的掩码。与目的地址一起来标识目的主机或路由器所在的网段的地址。 说明： 当目的 IP 地址和掩码均为 0.0.0.0 时，配置的为设备的缺省路由，即当查找路由表失败后，根据缺省路由进行包的转发。
网关	该路由的网关地址，通常为下一跳路由器的入口 IP 地址。 说明： 添加静态路由时，网关和接口必须指定其中的一个，否则无法添加成功。
接口	指定数据报文从安全网关的哪个接口或 ADSL 链路进行转发。 可以选择物理接口、VLAN 虚接口、GRE 虚接口、IPSecVPN 虚接口、SSLVPN

参数	说明
	虚接口、链路聚合虚接口； 也可以指定出接口的属性，可选项为 adsl、adsl1、adsl2 和 adsl3，用于指定数据报文从哪条 ADSL 链路进行转发。 说明： 添加静态路由时，“网关”和“接口”必须指定其中的一个，否则无法添加成功。
度量值	设置路由的优先级，值越小，优先级越高。默认为 1，取值范围为 1-65535。 说明： 当同一目的地存在多条静态路由时，优先级高的路由将成为当前的最优路由。
权重值	设置该静态路由的权重值。默认为 1，取值范围为 1-128。 说明： 1) 权重值越大，静态路由的优先级越高。 2) 如果静态路由表中存在多个“度量值”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。
探测 ID	选择已经设置的探测链路的 ID 号。如果不选择，则不进行探测。 说明： 1) 如果选择的链路状态显示为“链路不可达”，则新添加的静态路由的“标记”一栏不显示“U”，表示该条路由不可用。 2) 如果在静态路由中引用了某IP探测的“ID号”，并且在命令行下使用命令 #network route ipprobe on 开启路由探测功能，那么静态路由模块会根据IP探测的结果作为路由是否可用的依据。如果不开启路由探测功能，则此处选择的探测ID无效，将不对链路进行探测。

b) 设置完成后，点击“确定”按钮添加静态路由，也可点击“取消”取消添加并返回上一界面。

4) 删除静态路由

对于手工添加的静态路由，可以选择该路由由所在行的删除图标删除该条静态路由，也可以点击“清空”按钮，一次性删除所有手工添加的静态路由。

6.4.2 策略路由

策略路由不仅能够根据目的地址，而且能够根据协议类型、应用、IP 源地址或者其它的条件来确定报文的转发路径。策略路由的优先级高于普通路由。

在网络卫士安全网关系统中，策略路由分为两类：

➤ 入接口策略路由

与接口同名属性对象绑定的策略路由，用于匹配从相应接口传入设备且需设备转发的报文。

➤ 全局策略路由

与 global 属性绑定的策略路由，用于匹配经过设备需要转发的报文。匹配时，首先检查入接口策略路由中是否有匹配项，没有匹配项时再检查属性为 global 的策略路由。

本节介绍策略路由的相关配置：包括策略路由的添加、删除、清空操作，以及通过移动来改变策略路由中路由条目的默认排列顺序。

说明

- ✧ 在默认情况下，静态路由和策略路由条目一共最多可以添加 800 条，此数目可以通过购买 licence 进行扩展。如果添加时候策略路由已经超过了允许的最大值，则系统会返回已达上限的错误。

策略路由在网络卫士安全网关上的设置步骤如下：

- 1) 在左侧导航菜单中选择 **网络管理 > 路由**，点击“策略路由”页签，可以看到策略路由表，如下图所示。

路由表	策略路由	动态路由OSPF	动态路由RIP	动态路由BGP	多播路由
标记: U-Up, G-Gateway specified, i-Interface specified					
+ 添加 清空 总计: 0					
名称	入接口	操作			
eth0_policy	eth0	+ -> ->			

- 2) 添加策略路由

所有本机发出的策略路由、接口的策略路由和全局的策略路由只能添加一条，添加第二条时会有错误提示信息，并会添加一条没有绑定属性的空的策略路由。

- a) 点击“添加”，添加一条空的策略路由，如下图所示。

添加策略路由

名称

绑定

☐ 全局
 ☒ 入接口

可用接口

eth0
eth1
eth2
eth3
ipsec0

->
X

已选接口

确定

取消

参数说明如下表所示：

参数	说明
名称	输入字符作为策略路由的唯一标识，不得与已有策略路由名相同，而且不得超过 31 个字符，否则会提示错误信息。
属性绑定	选择此策略绑定的属性，可选择一个或多个。属性分为三类：local、global，以及接口相关的属性，例如 eth0。 说明：

参数	说明
	1) 当选择“入接口”时，需要选择绑定的属性。由于接口和属性是一一对应的，因此将策略与属性绑定实现了策略与接口的绑定，从而使得不同的接口收到的数据包可以使用不同的路由策略。 “入接口”指的是接收数据报文的接口，可以为任何接口，但是只有可以路由的接口才会起作用，可以路由的接口包括：非交换模式的物理接口、VLAN 虚接口、子接口以及 ipsec、GRE 等动态接口。 2) 当属性选择“全局”时，添加全局的策略路由。任何接口收到的数据包都会查找全局的策略路由。 3) 如果全局的策略路由和接口相关的策略路由定义相冲突，则全局策略路由的优先级低于接口相关的策略路由。

b) 点击“确定”，添加一条策略路由。

3) 添加具体的匹配策略

a) 点击“操作”一栏的“+”图标，管理员可以向策略路由中添加新的策略路由条目。界面如下图所示。

添加路由条目

源地址	
源掩码	
目的地址	
目的掩码	
网关	
接口	-选择接口-
▼ 高级	
源端口	- [0-65535; 单个端口只填起始端口]
目的端口	- [0-65535; 单个端口只填起始端口]
协议	-选择协议-
度量值	[1-65535]
权重值	[1-128]
确定 取消	

各参数的具体说明请参见下表。

参数	说明
源地址	用来标识 IP 包的源地址或源网络。注意填写源地址转换前的 IP 及掩码，也就是真实的子网地址。
源掩码	源 IP 地址的掩码。与源地址一起来标识源主机或路由器所在的网段的地址。
目的地址	用来标识 IP 包的目的地址或目的网络。需要填写目的地址转换后的真实地址。
目的掩码	目的 IP 地址的掩码。与目的地址一起来标识目的主机或路由器所在的网段的地址。
网关	该路由的网关地址，通常为下一跳路由器的入口 IP 地址。

参数	说明
接口	指定数据报文从安全网关的哪个接口转发出去。
源端口	标识数据包的源端口的范围，如果为单个端口，则只填写起始端口即可。默认是所有端口。
目的端口	标识数据包的端口的范围，如果为单个端口，则只填写起始端口即可。默认是所有端口。
协议	通过下拉框选择数据包使用的协议。
度量值	接口跃点数，默认为 1，取值范围为 1-65535，度量值的大小定义了路由的优先级，度量值越小，优先级越高。
权重值	设置该策略路由的权重值。默认为 1，取值范围为 1-65535。 说明： 如果策略路由表中存在多个“度量值”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。

b) 设置完成后，点击“确定”按钮完成策略路由条目的添加，也可点击“取消”取消添加并返回上一界面。

c) 点击某条策略路由左侧的“▶”按钮，可以查看其中的策略路由条目。

路由表

策略路由

动态路由OSPF

动态路由RIP

动态路由BGP

多播路由

标记: U-Up, G-Gateway specified, i-Interface specified

+ 添加

🗑️ 清空

总计: 1

▶ 名称		入接口		操作								
▼ eth0_policy		eth0		+📄🔗								
路由ID	源	目的	源端口	目的端口	协议	网关	度量值	权重值	接口	标记	移动	删除
100	10.10.10.9/32	172.16.1.9/32				0.0.0.0	1	1	eth1	i	📁	🗑️

点击“名称”左侧的“▶”按钮，则将所有路由条目展开显示。

路由表		策略路由		动态路由OSPF		动态路由RIP		动态路由BGP		多播路由		
标记: U-Up, G-Gateway specified, i-Interface specified												
+ 添加 清空										总计: 2		
▼名称		入接口				操作						
▼ eth0_policy		eth0				+  						
路由ID	源	目的	源端口	目的端口	协议	网关	度量值	权重值	接口	标记	移动	删除
100	10.10.10.9/32	172.16.1.9/32				0.0.0.0	1	1	eth1	i		
▼ eth2_policy		eth2				+  						
路由ID	源	目的	源端口	目的端口	协议	网关	度量值	权重值	接口	标记	移动	删除
101	192.168.83.0/32	172.16.0.0/32				192.168.83.1	1	1	eth0	UGi		

d) 由于策略路由执行顺序匹配原则，管理员可以通过移动来调整策略路由的默认添加顺序。移动策略的具体设置方法为：

在策略路由表中点击要移动的路由选项（例如要移动策略路由 102）后的移动图标“[icon]”，进入如下界面。



在第一个下拉框中选择参考位置路由的 ID 号，第二个下拉框中则是选择将当前路由移动到参考路由之前还是之后。点击“确定”按钮，完成移动操作。

e) 点击路由条目对应的删除图标，可删除该路由条目。

4) 删除策略路由

在策略路由界面中，用户点击策略路由对应的删除图标，可以删除该策略路由。点击“清空”按钮则可一次性删除所有的策略路由。

6.4.3 动态路由 OSPF

OSPF 协议是一个基于链路状态的动态路由协议，它通过收集和传递自治系统的链路状态来动态地发现并传播路由。网络卫士安全网关支持 OSPF 协议版本 2。

说明

- ✧ 网络卫士系列安全网关逻辑上支持 50 个接口运行 OSPF 协议。
- ✧ 通过 WEBUI 只可以配置基本的 OSPF 路由选项。其他选项只有通过 CLI 命令配置。有关使用 CLI 命令配置 OSPF 设置的详细信息，参见《网络卫士安全网关命令行手册——基础配置》中“OSPF”章节。

6.4.3.1 启动或停止 OSPF 服务

在设备上如果要运行 OSPF 协议，则必须首先启用 OSPF 进程。

启动 OSPF 进程的具体操作如下：

1) 选择 **网络管理 > 路由**，并选择“动态路由 OSPF”页签，界面如下图所示。



2) 启动 OSPF 进程

点击“启动”按钮便可启动 OSPF 进程。只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。启动后界面如下图所示。

动态路由OSPF 动态路由RIP 动态路由BGP 多播路由

OSPF设置

启动 停止 查看

route-id 设置 重启

区域配置 +添加

运行网段	区域ID	删除

路由重发布 设置

缺省路由重发布 设置

acl +添加

名称	运行网段	权限	删除

acl分发 +添加

名称	路由类型	删除

接口设置 +添加

接口名称	修改

3) 停止 OSPF 进程

点击“停止”按钮即可停止 OSPF 进程运行，同时设置的 OSPF 协议的相关参数也随之丢失。

4) 重启 OSPF 服务

当网络在当前运行的 OSPF 协议下出现某些不良状况，重启 OSPF 进程可以达到改善网络运行状况的目的。点击“重启”按钮，重新启动 OSPF 进程，如下图所示。

route-id 设置 重启

说明

- ✧ 重启 OSPF 进程与停止 OSPF 进程最根本的区别在于，重启 OSPF 进程可以不改变 OSPF 协议的参数配置。

6.4.3.2 查看 OSPF 协议配置信息

点击“查看”按钮，弹出查看界面，可以查看 OSPF 路由协议的运行状况，包括 OSPF 当前的状态信息、数据链路状态数据库中的 LSA 信息、OSPF 协议运行接口的信息、OSPF 协议邻居信息和 OSPF 协议的路由信息，如下图所示。



各按钮的功能说明如下表。

按钮	说明
查看配置	点击此按钮后，会在下面的文本框中显示 OSPF 当前的所有配置信息。
查看数据库	点击此按钮后，会在下面的文本框中显示 OSPF 数据库信息，包括区域 ID、路由器 IP 等信息。
查看接口	点击此按钮后，会在下面的文本框中显示各接口的情况，包括是否激活、是否启用 OSPF 等。
查看邻居	点击此按钮后，会在下面的文本框中显示相邻的其他路由设备的信息。
查看路由	点击此按钮后，会在下面的文本框中显示 OSPF 路由信息。
查看调试	点击此按钮后，会在下面的文本框中显示 OSPF 的协议的调试信息。
返回	点击此按钮后，会返回 OSPF 设置主界面。

6.4.3.3 配置路由 ID

本节介绍如何设置 OSPF 协议要通告的网络路由号 route-id。因为环回接口性能稳定，在网络出现状况时不易受到影响，所以通常设置环回地址作为 OSPF 协议中的 route-id。

在“OSPF 协议路由配置”处可以设置 OSPF 协议要通告的 route-id 号，如下图所示。

route-id		设置	重启

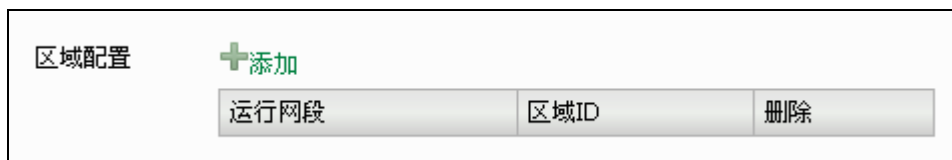
输入环回地址作为网络路由号 route-id，点击“设置”按钮使设置生效。

6.4.3.4 设置区域

启动 OSPF 进程后，设定运行 OSPF 协议的网段以及该网段所属的 OSPF 区域。

区域信息配置具体设置方法如下：

1) OSPF 区域配置界面如下图所示。



该截图显示了 OSPF 区域配置界面。顶部有一个“区域配置”标题，右侧有一个绿色的“+添加”按钮。下方是一个表格，包含三列：运行网段、区域ID 和 删除。

2) 添加区域网络

可以添加多个区域网络，但是一个网段只能属于一个区域。

a) 点击“区域配置”右侧的“添加”按钮，进入设置“OSPF 区域”页面，如下图所示。



该截图显示了“OSPF 区域”设置对话框。对话框顶部有“OSPF 区域”标题。下方有两个输入框：第一个是“运行网段”，格式为“IP地址/掩码”，右侧有红色星号标注“* [子网/掩码]”；第二个是“区域ID”，右侧有红色星号标注“* [0-4294967295]”。底部有两个按钮：“确定”和“取消”。

输入运行 OSPF 协议的网段 IP 地址和掩码，以及网段所属区域 ID。

b) 点击“确定”完成区域设定。

3) 删除区域网络

对于已经添加的 OSPF 区域，可以通过点击对应的“删除”按钮进行删除。

4) 重新启动相关接口

设置完成后，需要将应用 OSPF 协议的接口重新启动，保证该接口可以正确通告 OSPF 路由。接口重新启动请参见[6.2.1 物理接口](#)的相关内容。

6.4.3.5 重新发布路由

网络卫士安全网关 OSPF 支持将本地路由表中的直连、BGP、RIP、静态等路由重新发布到 OSPF 自治系统。发布的静态路由包含缺省路由。

➤ 路由重发布

1) 在“动态路由 OSPF”标签页中“路由重发布”处进行设置。界面如下图红框所示。



2) 点击“设置”按钮，进入重发布信息设置页面，如下图。

3) 选择要重新发布的路由类型，勾选“启动”后，将对路由表中的该类路由重新发布。

如果管理员在其后的文本框中设置数值，则邻居引入该路由后将标记此处设置的“度量值”。否则，将按照“缺省度量值”处设置的数值作为其度量值。

4) 点击“确定”，该页面配置参数生效。点击“取消”放弃参数修改并返回上一界面。

➤ 缺省路由重发布

1) 在“动态路由 OSPF”标签页中“缺省路由重发布”处进行设置。界面如下图红框所示。



2) 点击“设置”按钮，进入缺省路由重发布信息设置页面，如下图。

- 3) 设置缺省路由的开销后，勾选“启动”，将缺省路由重新发布。
- 4) 点击“确定”，该页面配置参数生效。点击“取消”放弃参数修改并返回上一界面。

6.4.3.6 设置 ACL

ACL 规则用于定义对重新发布到 OSPF 的路由更新信息进行筛选的条件。ACL 规则本身不能对路由更新信息进行过滤，只有将 ACL 规则应用到 ACL 分发规则，才可以对重新发布到 OSPF 系统的路由更新信息进行过滤。

说明

- ✧ 此处的ACL不同于防火墙模块的访问控制规则，防火墙模块的访问控制规则用于过滤穿越设备的流量，对于设备自身产生的流量信息（例如路由更新报文）不起作用。而此处的ACL规则用于过滤路由更新报文。

定义 ACL 规则的具体步骤为：

- 1) 在“ACL”处设置访问控制规则，界面如下图所示。

acl

+

添加

名称	运行网段	权限	删除
deny	10.10.10.0/24	deny	
deny	11.11.11.0/24	deny	
permit	192.168.83.0/24	permit	

所有规则均按照添加顺序进行排列，引用规则的 ACL 分发规则将按照规则的排列顺序进行匹配，按照最先匹配的规则权限对路由更新报文进行处理。如果没有满足任何一条规则，则根据默认权限禁止路由更新。

- 2) 添加访问控制规则

点击“添加”，界面如下图所示。

OSPF访问控制配置

名称

*

运行网段

/

* [子网/掩码]

权限

☒ 允许
 ☐ 拒绝

确定

取消

界面中参数说明如下表所示。

参数	说明
名称	输入 ACL 规则名称。 说明： 可以是已经添加的规则名称，此时，该规则中包含多个表项，按照添加顺序排列，排列在前面的规则具有优先权。
运行网段	设置路由过滤的子网 IP 及其掩码。
权限	“允许”或“拒绝”“运行网段”指定的路由更新信息重新发布到 OSPF 自治系统。

点击“确定”，完成 ACL 规则配置。

3) 删除访问控制规则

通过点击“删除”按钮，指定相同的参数，可以删除访问控制规则。

6.4.3.7 设置 ACL 分发规则

缺省情况下，OSPF不对重新发布的路由信息进行过滤。通过定义ACL规则（请参见[6.4.3.6设置ACL](#)），然后在ACL分发规则中引用ACL规则，对重新发布到OSPF自治系统中的其他类型的路由条目进行过滤，达到控制路由更新的目的。

设置界面如下图所示。

acl分发
+添加

名称	路由类型	删除

1) 添加分发规则

点击“添加”按钮，界面如下图所示。

OSPF分发配置

名称

路由类型

界面中参数说明如下表所示。

参数	说明
名称	输入所引用的 ACL 规则名称。对于符合规则的路由更新，会根据 ACL 规则定义的权限允许或拒绝被重分发到 OSPF。 说明： 1) 要想规则生效，管理员必须设置同名的 ACL 规则。 2) 当 ACL 列表中有多个同名的规则时，系统将按照最先匹配的规则的权限处理重新发布的路由信息。

参数	说明
路由类型	根据“访问控制规则”设置的权限，选择需要重分发到 ospf 的路由协议的类型，有 4 个可选项：connected、bgp、rip 和 static。其中 connected 表示直连路由，bgp 表示 BGP（边界网关协议）路由，rip 表示 RIP 路由，static 表示静态路由。

点击“确定”，完成 OSPF 分发规则配置。

2) 删除分发规则

设置完成分发规则后，还可以通过点击“删除”图标删除分发规则。

6.4.3.8 设置接口属性

在网络卫士安全网关上，允许管理员修改指定接口的 OSPF 协议参数，以保证某些参数在相连网络的所有路由器上保持一致。

具体设置为：

1) 在“动态路由 OSPF”标签页中“OSPF 协议接口设置”处可以对 OSPF 协议的接口进行设置，如下图所示。

2) 设置接口的 OSPF 协议参数

管理员可以根据需要改变任何参数值，但必须保证“认证方式及其口令”和“发送 HELLO 报文时间间隔”在相连网络的所有路由器上保持一致。

a) 点击“添加”，界面如下图所示。

页面上各参数的说明如下表。

参数	说明

参数	说明
接口	指定配置哪个接口的 OSPF 认证参数的属性。
认证方式	设置通过该接口进行链路状态通告（LSA）互换时验证的方式。可以选择明文、MD5 或不认证。缺省情况下不进行认证。 设置为“不认证”时不进行身份验证。 设置为“明文”时，使用基于存文本的密码方式验证 LSA。 设置为“MD5”时，使用 MD5 认证方式验证 LSA。 说明： 一个区域内所有的路由器接口必须使用相同的身份验证方法。
认证口令	配置接口采用明文或 MD5 认证时使用的口令。 说明： 一个区域内所有的路由器接口必须使用相同的口令。
接口开销	配置该接口的开销。范围为 1-65535，缺省值 10。
发送 HELLO 报文间隔	配置通过该接口发送 hello 报文的时间间隔。单位是秒，缺省情况下是 10 秒。范围为 1-65535。

b) 点击“确定”完成参数设置。

3) 修改接口属性

设置完接口属性后，还可以通过点击“修改”图标修改属性。

6.4.4 动态路由 RIP

RIP 是一种距离向量协议，网络卫士安全网关支持 RIP 协议的 v1、v2 版本。

说明

- ◇ 通过 WEBUI 只可以配置基本的 RIP 路由选项。其他选项只有通过 CLI 命令配置。有关使用 CLI 命令配置 RIP 设置的详细信息，参见《网络卫士安全网关命令行手册——基础配置》中“RIP”章节。

6.4.4.1 启动或停止 RIP 协议

在设备上如果要运行 RIP 协议，则必须首先启用 RIP 进程。

启动 RIP 进程的具体操作如下：

- 1) 选择 **网络管理 > 路由**，并选择“动态路由RIP”页签，界面如下图所示。



- 2) 启动 RIP 进程

点击“启动”按钮便可启动 RIP 进程。只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。启动后界面如下图所示。



2) 点击“停止”按钮可停止 RIP 进程。

6.4.4.2 查看 RIP 协议配置信息

点击“查看”按钮，弹出查看界面，管理员可以查看 RIP 路由协议的运行状况，包括 RIP 当前的状态信息、当前的配置信息、RIP 路由信息和 RIP 协议的调试信息。如下图所示。



各按钮的功能说明如下表。

按钮	说明
查看配置	点击此按钮后，会在下面的文本框中显示当前路由器的运行状态信息，例如是否启动了 RIP 协议、以及设置的其他参数值。
查看状态	点击此按钮后，会在下面的文本框中显示当前路由器的运行状态信息，例如是否启动了 RIP 协议、启动 RIP 协议的端口信息等。

按钮	说明
查看路由	点击此按钮后，会在下面的文本框中显示 RIP 路由信息。
查看调试信息	可以查看调试 RIP 协议详细的历史信息，例如各 RIP 路由接口发送、接收 RIP 路由的信息等。
取消	点击此按钮后，会返回 RIP 设置主界面。

6.4.4.3 设置网络

由于 RIP 协议使用广播进行报文发送，本节主要定义运行 RIP 协议的网段。RIP 任务启动后必须指定其工作网段。RIP 只在指定网段的接口上运行；对于不在指定网段上的接口，RIP 既不在它上面接收和发送路由，也不将它的接口路由转发出去，就好像这个接口不存在一样。

1) 在“网络配置”处可以设定 RIP 区域，如下图所示。

网络配置

运行网段	删除
192.168.83.0/24	

2) 添加网络

点击“添加”按钮，出现“RIP 区域”页面，如下图所示。

RIP 区域

运行网段 / * [子网/掩码]

确定 取消

输入运行 RIP 协议的网段 IP 地址和掩码，单击“确定”，完成设置。

2) 删除网络配置

点击某网段对应“删除”图标，可以删除该网段。

6.4.4.4 设置邻居

在某些非广播网络上，比如 X.25、帧中继网络上，可以通过指定邻居 IP 地址的方式让 RIP 发送单播地址报文。我们的设备接口都是以太网口为广播网络，也可以使用单播向指定的邻居发送路由更新信息。

设置邻居包括添加和删除邻居的配置信息。具体步骤如下：

1) 在邻居处进行设置，界面如下图所示。

邻居配置

+

添加

IP

删除

2) 添加邻居

点击“添加”按钮，进入如下页面。

RIP邻居IP配置

IP地址

*

确定

取消

在文本框中填写邻居路由器的 IP 地址，点击“确定”即可。

3) 删除指定的邻居

点击某邻居对应的“删除”图标，可以删除指定邻居。

6.4.4.5 重新发布

网络卫士安全网关支持将本地路由表中的直连、OSPF、静态等路由重新发布到 RIP 路由协议中。

1) 在“重新发布信息”处进行配置，如下图所示。

路由重发布

设置

2) 点击“设置”按钮，右侧界面如下图所示。

RIP重新发布配置

已连接度量值

☐ [1-16]

OSPF度量值

☐ [1-16]

静态度量值

☐ [1-16]

默认跳数

[1-16]

确定

取消

界面中参数说明如下表所示。

参数	说明
已连接度量值	表示要将直连的路由信息引入到 RIP 路由中作为外部路由信息，并可在其后的文本框中设置路由引入后的 metric 值。取值范围为 1-16。

参数	说明
OSPF 度量值	表示要将 OSPF 的路由信息引入到 RIP 路由中,并可在其后的文本框中设置路由引入后的 metric 值。取值范围为 1-16。
静态度量值	表示要将静态的路由信息引入到 RIP 路由中,并可在其后的文本框中设置路由引入后的 metric 值。取值范围为 1-16。
默认跳数	表示默认引入路由的跳数。在引入路由时,如果不分别指定各类型路由的 metric 参数,则使用默认路径开销作为路由引入后的跳数。取值范围为 1-16。

3) 点击“确定”，该页面配置参数生效。

6.4.5 动态路由 BGP

BGP（边界网关协议）是为 TCP / IP 互联网设计的外部网关协议，主要功能是在自治系统间传递路由信息，它的功能不在于发现和计算路由，BGP 传递的路由信息需要注入。网络卫士安全网关提供对 BGP 协议的支持。

BGP 的基本配置有 3 步：

（1）启动 BGP 协议；（2）配置 BGP 邻居；（3）为 BGP 注入路由信息；

网络卫士安全网关支持通过宣告网段、通过路由重发布、通过地址聚合通告汇总地址三种方法向 BGP 注入路由信息。

具体配置步骤为：

选择 **网络管理 > 路由**，并选择“动态路由BGP”页签，设置BGP动态路由协议的相关参数，界面如下图所示。

6.4.5.1 启动或停止 BGP 协议

网络卫士安全网关在缺省情况下不运行BGP。在使用BGP协议之前，需要首先启用BGP进程。启动BGP后，本地的BGP进程开始监听相邻路由器的BGP连接请求。要使本地BGP进程主动向相邻路由器发出BGP 连接请求，请参见 [6.4.5.5邻居](#)。

1) 启动 BGP 协议

在上图中的“设置 AS 号”处设置 BGP 协议的本地自治系统号，范围为 1 到 65535，之后点击“启动”按钮启动 BGP 协议。

启动 BGP 进程后，管理员才可进行相关配置信息的查看和设置。如下图所示。

BGP设置

自治系统号

[1-65535]

启动

停止

查看

router-id

设置

宣告网段

+添加

宣告网段	删除

邻居

+添加

IP地址	自治系统号	编辑	删除

重新发布路由到BGP

设置

地址聚合

+添加

地址	带有自治系统号	只发送聚合路由	删除

2) 停止 BGP 进程

点击“停止”按钮，可以停止 BGP 进程的运行，BGP 将切断所有已经建立的 BGP 连接。

6.4.5.2 查看 BGP 协议配置信息

启动 BGP 进程后，点击“查看”按钮可以查看 BGP 路由协议的运行状况，包括 BGP 当前的状态信息、路由表条目、BGP 摘要信息和 BGP 协议的邻居状态信息。如下图所示。

BGP协议配置信息

当前配置

路由表条目

BGP摘要

邻居状态

network bgp start as 2
network bgp router-id 10.10.10.1

返回

各按钮的功能说明如下表。

按钮	说明
当前配置	点击此按钮后，会在下面的文本框中显示当前路由器的运行状态信息，例如是否启动了 BGP 协议、启动 BGP 协议的 AS 号等。
路由表条目	点击此按钮后，会在下面的文本框中显示 BGP 的路由详细信息。
BGP 摘要	点击此按钮后，会在下面的文本框中显示 BGP 的路由的简单摘要信息。
邻居状态	点击此按钮后，会在下面的文本框中显示 BGP 的所有邻居详细信息。
返回	点击此按钮后，会返回 BGP 设置主界面。

6.4.5.3 配置路由 ID

本节介绍如何设置 BGP 协议要通告的网络路由号 route-id，为了达到网络路由号能够唯一地标识本地路由器的目的，route-id 应设置为路由器的 IP 地址。

在“BGP 协议路由配置”处可以设置 BGP 协议要通告的 route-id 号，如下图所示。

The screenshot shows a configuration field labeled 'router-id' with an adjacent input box and a button labeled '设置' (Set).

输入路由器的 IP 地址作为路由 ID，点击“设置”按钮使设置生效。

6.4.5.4 宣告网段

网络卫士安全网关支持从 IP 路由表中取出本地连接的路由、静态路由或 IGP 路由，并注入到本地 BGP 表中。通过配置“宣告网段”，系统在设备的当前 IP 路由表中查找与“宣告网段”精确匹配的路由，注入本地 BGP 表。

宣告网段的设置方法如下：

- 1) 在“宣告网段”处进行配置，如下图所示。

The screenshot shows a configuration area titled '宣告网段' (Announce Segment). It includes a green '+添加' (Add) button and a table with two columns: '宣告网段' (Announce Segment) and '删除' (Delete).

- 2) 添加宣告网段

点击“添加”，界面如下图所示。

The screenshot shows a dialog box titled 'BGP宣告网段' (BGP Announce Segment). It contains a field for '宣告网段' (Announce Segment) with a placeholder for IP address and subnet mask, followed by a red asterisk and the text '[子网/掩码]' (Subnet/Mask). At the bottom, there are two buttons: '确定' (Confirm) and '取消' (Cancel).

设置子网地址及其掩码后，点击“确定”按钮完成设置。

3) 删除网段

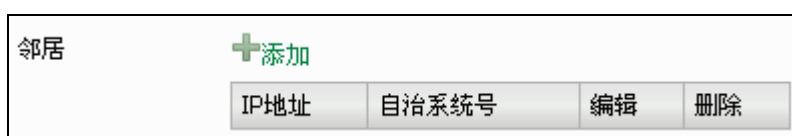
对于已经添加的宣告网段，可以点击“删除”图标进行删除。

6.4.5.5 邻居

这里的“邻居”是指在网络中与本地路由器相邻的其他路由器，系统支持添加和删除邻居信息，邻居信息的设置包括设置邻居的 IP 地址、AS 号、md5 密钥、next-hop-self、default-originate 选项。

邻居的设置方法如下：

1) 在“邻居”处进行配置，如下图所示。



邻居配置界面截图，显示“邻居”标题，右侧有“+添加”按钮。下方有四个按钮：IP地址、自治系统号、编辑、删除。

2) 添加 BGP 邻居

点击“添加”进入邻居设置界面，如下图所示。



BGP邻居基本配置界面截图，包含以下配置项：

- 邻居IP地址：输入框，右侧有红色星号 *
- 邻居自治系统号：输入框，右侧有红色星号 * 和范围 [1-65535]
- 强制下一跳：复选框
- 宣告缺省路由：复选框
- 邻居MD5认证密钥：输入框，右侧有提示 [最多20个字符]

底部有“确定”和“取消”按钮。

参数说明如下表所示：

参数	说明
邻居 IP 地址	邻居的 IP 地址即是相邻路由器的网络路由号 route-id。
邻居自治系统号	指定 BGP 邻居所属的 AS 号。
强制下一跳	配置在发布路由时是否将自身地址作为下一跳。BGP 路由器向对等体组发布路由时，可使用自身地址作为下一跳。 缺省情况下，本地路由器向对等体组发布路由时不把自身地址作为下一跳。
宣告缺省路由	设置同伴组是否引入默认路由，缺省不引入。
邻居 MD5 认证密钥	设置 BGP 邻居之间进行 MD5 认证的密码。 说明：

参数	说明
	BGP 对等体/对等体组之间需要建立并保持 TCP 连接，为提高 BGP 的安全性，可以配置在建立 TCP 连接时进行 MD5 认证，如果认证失败，则不能建立 TCP 连接。BGP 的 MD5 认证功能并不对 BGP 报文进行认证，它只是为 TCP 连接设置一个 MD5 认证密码，由 TCP 完成认证。

点击“确定”，该页面配置参数生效。点击“取消”放弃参数修改并返回上一界面。

3) 对于已经添加的邻居信息，可以点击“编辑”图标进行修改；也可以点击“删除”图标将其删除。

6.4.5.6 重新发布信息

网络卫士安全网关支持将本地路由表中的静态、直连、RIP 或者 OSPF 的路由信息重新发布向本地 BGP 表中注入路由。

1) 在“重新发布信息”处进行配置，如下图所示。



2) 点击“设置”按钮，右侧界面如下图所示。

重新发布信息

OSPF度量值		[0-16777214]	☐	启动
直连度量值		[0-16777214]	☐	启动
RIP度量值		[0-16777214]	☐	启动
静态度量值		[0-16777214]	☐	启动

界面中参数说明如下表所示。

参数	说明
OSPF 度量值	表示是否要将 OSPF 的路由信息引入到 BGP 路由中，并可在其后的文本框中设置路由引入后的 metric 值。取值范围为 0-16777214。选择“启用”表示引入。
直连度量值	表示是否要将直连的路由信息引入到 BGP 路由中作为外部路由信息，并可在其后的文本框中设置路由引入后的 metric 值。取值范围为 0-16777214。选择“启用”表示引入。
RIP 度量值	表示是否要将 RIP 的路由信息引入到 BGP 路由中，并可在其后的文本框中设置路由引入后的 metric 值。取值范围为 0-16777214。选择“启用”表示引入。
静态度量值	表示是否要将静态的路由信息引入到 BGP 路由中，并可在其后的文

参数	说明
	本框中设置路由引入后的 metric 值。取值范围为 0-16777214。选择“启用”表示引入。

3) 点击“确定”，该页面配置参数生效。点击“取消”放弃参数修改并返回上一界面。

6.4.5.7 地址聚合

“地址聚合”用于配置 BGP 的路由聚合功能，就是把各段路由综合到一个或多个聚合或 CIDR 中，以便把路由表中的路由数目减到最小。BGP 路由聚合有两种方式：自动聚合 summary 与手动聚合 aggregate。自动聚合 summary 是对 BGP 引入的 IGP 子网路由进行聚合。配置 summary 后，BGP 将不能接收从 IGP 引入的子网路由。手动聚合 aggregate 是对 BGP 本地路由进行的聚合。在手动聚合方式下可配置一系列参数。通常情况下，手动聚合的优先级要比自动聚合的优先级高。

地址聚合的设置方法如下：

1) 在“地址聚合”处进行配置，如下图所示。

地址聚合
+ 添加

地址
带有自治系统号
只发送聚合路由
删除

2) 添加策略

点击“添加”设置聚合策略，界面如下图所示。

BGP地址聚合

聚合网段
 / * [子网/掩码]

带有自治系统号

只发送聚合路由

确定
取消

参数说明如下表所示：

参数	说明
聚合网段	设置进行地址聚合的网段地址及其子网掩码。
带有自治系统号	设置是否为带有自治区号的路由进行聚合。
只发送聚合路由	设置是否只发送聚合路由略去原路由。设置为“开”时将只发送聚合路由略去原路由；设置为“关”时将聚合路由和原详细路由都通告给

参数	说明
	对等体。

点击“确定”，该页面配置参数生效。点击“取消”放弃参数修改并返回上一界面。

3) 删除策略

对于已经添加的地址聚合策略，可以点击“删除”图标进行删除。

6.4.6 多播路由

当网络卫士安全网关工作在路由模式时，通过定义静态多播路由，允许特定多播组的IP多点广播数据报文穿越网络卫士安全网关。

定义多播路由的具体操作方法如下：

1) 选择 **网络管理 > 路由**，并在右侧页面选择“多播路由”页签，进入多播路由设置页面，如下图所示。

2) 添加多播路由

点击“添加”，系统进入多播路由表项配置页面，如下图所示。

各参数的含义如下。

参数	说明

参数	说明
源地址/源掩码	指定多播服务器所在的地址或地址段。如果配置为 0.0.0.0/0，则指所有地址。
多播组	多播组的 IP 地址。
多播流量源接口	限定多播流量的来源接口。
发送加入报告	选择该项后，网络卫士安全网关可以在目的接口有下游多播路由器的情况下，由安全网关设备定时地向上游多播路由器发送加入报告（Joining Report），以保证多播报文顺利地转发给下游多播路由设备，维护多播树结构。
目的接口	选择多播流量转发的目的接口。目的接口与源接口不能相同。

点击“确定”，完成多播路由的设置。

3) 删除多播路由

对于已有路由，管理员可以点击对应的“删除”图标删除一条多播路由，或点击“清空”一次性删除所有多播路由。

6.5 接入

主要介绍如何设置 ADSL 连接、虚拟转发线路、聚合链路、802.1X 认证和 VLAN-VPN 的相关参数。

6.5.1 ADSL

当企业内网用户利用 ADSL 接入方式连接 Internet 时，网络卫士安全网关可以配置为 PPPoE 客户端，通过外接 ADSL Modem，拨号与远端的 ADSL 服务器建立 PPPoE 连接。局域网内的主机不用安装 PPPoE 客户端软件即可访问 Internet，而且同一个局域网中的所有 PC 可以共享一个 ADSL 帐号。

安全网关支持两种 ADSL 连接方式：主动连接方式和按需拨号方式。

- 主动连接方式：根据管理员启动或停止拨号的指令，建立或断开内外网之间的通信链路。拨号连接建立后，除非管理员主动停止拨号连接，否则此 PPPoE 会话将一直存在。
- 按需拨号方式：系统根据流量信息控制拨号过程。只有当有数据需要传送时，安全网关才会发起 PPPoE 呼叫，建立 PPPoE 会话。如果 PPPoE 链路的空闲时间超过用户的配置，安全网关会自动中止 PPPoE 会话。

网络卫士安全网关支持多路拨号功能，最多可以提供 4 条 ADSL 拨号链路，可以有效地扩充网络流量。如果管理员需要指定部分用户使用某条固定的链路连接外网，则需要设置“接口”属性为 ADSL 的静态路由，具体请参见 [6.4.1 路由表](#)。

ADSL 配置步骤如下：

1) 选择 **网络管理 > ADSL**，进入ADSL设置页面，如下图所示。

ADSL										
虚拟线		链路聚合		802.1x		VLAN-VPN				
链路名称	描述	状态	带宽	分配IP地址	对端IP地址	收到报文	发送报文	拨号持续时间	操作	设置属性
adsl		未连接								
adsl1		未连接								
adsl2		未连接								
adsl3		未连接								

网络卫士安全网关最多可以提供 4 条 ADSL 拨号链路，页面中显示了 ADSL 连接的当前状态。

2) 配置拨号参数

使用 ADSL 拨号之前，需要首先点击“设置属性”，设置 ADSL 拨号的相关参数，界面如下图所示。

ADSL属性

绑定属性

adsl

接口 ▼

eth0

用户名 *

密码 *

按需拨号

☐

高级

☒

MTU

1492 [1000-1492]

链路带宽

[1-1024Mbps, 默认单位KBps]

本地地址

度量值 (路由使用)

[1-65535]

权重值 (路由使用)

[1-128]

描述

确定

清除配置

取消

相关参数的说明如下表。

参数	说明
绑定属性	显示该接口绑定 ADSL 拨号属性。 说明： 物理接口与 ADSL 属性的绑定绝对不能在接口设置界面进行配置，否则会导致无法拨号成功。
接口	与 ADSL Modem 绑定的安全网关的以太网接口。
用户名/密码	指 ADSL 拨号时需要的用户名、密码，最多为 31 个字符，由运营商提供。

参数	说明
按需拨号	指是否选择按需拨号方式。 说明： 如果勾选“按需拨号”，参数设置完成就启动 ADSL 客户端进程。链路状态显示为“协商 pppoe 链路……”，当有流量通过 PPPoE 虚接口时，系统自动进行拨号。否则，需要点击“开始拨号”按钮才开始建立内外网之间的通信链路。
MTU	指拨号成功后的数据的最大传输单元，单位字节。默认为 1492 字节。范围为 1000-1492。
链路带宽	设置给该条 ADSL 链路分配的保证带宽。
本地地址	如果 ADSL 服务提供商支持给 ADSL 用户分配静态 IP 地址，则在本选项处需要输入此 IP 地址。否则为空即可。
度量值(路由使用)	设置该链路拨号成功后添加的默认路由的 Metric 值。默认为 1，取值范围为 1-65535。 说明： 1) Metric 值越小，静态路由的优先级越高。 2) 如果静态路由表中存在多个“Metric”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。 3) 如果管理员需要指定部分用户使用某条固定的链路连接外网，则需要设置 ADSL 静态路由，具体请参见 6.4.1 路由表。
权重值(路由使用)	设置该链路拨号成功后添加的默认路由的权重值。默认为 1，取值范围为 1-128。 说明： 1) 权重值越大，静态路由的优先级越高。 2) 如果静态路由表中存在多个“Metric”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。 3) 如果管理员需要指定部分用户使用某条固定的链路连接外网，则需要设置 ADSL 静态路由，具体请参见 6.4.1 路由表。
描述	可选项，输入对该链路必要的描述信息。

点击“清除配置”，则当前界面中的所有已经设置的参数均被删除。点击“取消”则对参数的设置或修改无效，返回主界面。

点击“确定”按钮完成参数设置。

需要说明的是：

a) 如果选择了“按需拨号”，则链路状态显示为“协商 pppoe 链路……”，“拨号状态”显示为“启动”状态仅表示安全网关上的 ADSL Client 进程处于启动状态，随时接听数据传输请求。当有数据需要通过 ADSL 链路传输时，安全网关才会发起 PPPoE 呼叫，建立 PPPoE 会话。

ADSL	虚拟线	链路聚合	802.1x	VLAN-VPN						
链路名称	描述	状态	带宽	分配IP地址	对端IP地址	收到报文	发送报文	拨号持续时间	操作	设置属性
adsl1		协商pppoe链路.....								
adsl11		未连接								
adsl12		未连接								
adsl13		未连接								

b) 如果没有选择“按需拨号”，则需要管理员点击页面上“操作”一列对应的启动按钮，发起 PPPoE 呼叫。“状态”一列会显示 ADSL 拨号协商的状况。

需要注意的是：

如果局域网内计算机使用的IP地址为私有地址，需要通过ADSL 链路访问外网时，还需要管理员在网络卫士安全网关上手工配置NAT源地址转换策略，将内网的数据报文的源地址转化为ADSL所绑定的属性名称，系统会自动将内网私有地址转换为属性所绑定的接口地址。同时，如果用户需要设置目的区域，则该目的区域必须与ADSL属性绑定。关于NAT地址转换规则的设定请参见9.4地址转换。

6.5.2 虚拟线

虚拟线（virtual-line）指的是在安全网关上设定一个物理接口组 AB 口，从 A 口进入安全网关后，除了目的地址为安全网关的数据报文外，均强制从 B 口进行转发，即不经二层交换以及三层路由的检查就将报文直接送出，相当于一个物理层交换机。

说明

- ✧ 虚拟线能够转发 802.1q 报文。
- ✧ 如果一个物理接口已经加入了端口聚合，则不能再加入虚拟线，因为端口聚合功能会在数据报文刚刚进入安全网关时将接收的物理接口替换为聚合后的虚拟聚合端口。
- ✧ 网络卫士安全网关不支持子接口之间建立虚拟线。
- ✧ 对于建立虚拟线的两个物理端口相关的 NAT 规则无效。
- ✧ 如果一个物理接口加入到虚拟线中，则数据将直接通过虚拟线转发，而不会通过虚接口转发，因此在 **虚拟专网 > 虚接口绑定** 处与该物理接口相关的绑定规则无效。
- ✧ 虚拟线对双机热备方式可以正常的支持，主设备和从设备的配置一致，在切换后仍然是按照虚拟线的方式在转发。虚拟线不支持 TOS 中 VRRP 方式的负载均衡，因为其是通过子接口实现的，虚拟线不支持子接口。
- ✧ 虚拟线的报文可以完全的支持阻断策略以及访问控制，因为这样的报文会正常的建立连接和维护连接，不会影响阻断策略的结果。
- ✧ 虚拟线不支持 AV 过滤和深度内容过滤，如果设置了虚拟线，在 ACL 规则中不应设置相关的 DPI 规则和 AV 策略。
- ✧ 虚拟线中的接口不支持 SYN 代理。

1) 设置虚拟线功能的方法是：选择 **网络管理 > 接入**，并激活“虚拟线”页签，如下图所示。

ADSL	虚拟线	链路聚合	802.1x	VLAN-VPN
+ 添加 清空				总计: 0
接口1	接口2	删除		

2) 添加虚拟线路

点击“添加”，增加新的虚拟线路，界面如下图所示。

虚拟线

接口1

-选择接口-

接口2

-选择接口-

确定

取消

在“接口1”和“接口2”处选择虚拟线路两端的物理接口名，点击“确定”后完成虚拟线路添加，添加成功后界面如下图所示。

ADSL	虚拟线	链路聚合	802.1x	VLAN-VPN
+ 添加 清空				总计: 1
接口1	接口2	删除		
eth2	eth3			

3) 删除虚拟线路

点击“删除”图标可以将已添加的虚拟线删除，点击“清空”按钮可以一次性将所有虚拟线全部删除。

6.5.3 链路聚合

网络卫士安全网关支持链路聚合功能，是将多个物理接口聚合成一个逻辑端口，聚合后的端口称为一条聚合链路，其性能接近各个网口的速率总和，可大大提高端口间的通信速度。该链路在逻辑上是一个整体，内部的组成和传输数据的细节对上层服务是透明的，聚合链路内部的物理链路共同完成数据收发任务并相互备份，只要还存在能正常工作的成员，整个传输链路就不会失效。网络卫士安全网关的链路聚合功能采用 802.3ad 的工作模式，聚合链路可以通过预先设置的负载均衡算法将流量分配给聚合链路内不同的物理接口，实现链路级的负载均衡功能，也可防止单条链路转发速率过低而出现丢包的现象。

在网络卫士安全网关上，加入到聚合端口中的接口限制为物理网口，不支持 vlan 等虚接口或子接口加入聚合端口中。而且参与聚合的物理接口必须具备相同的属性，如相同的速度、单双工模式等。如果物理接口在静态 ARP 表中有对应项，则该物理接口也无法

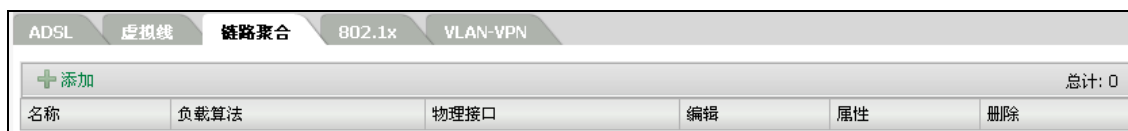
加入到 Bond 接口中。网络卫士安全网关将被聚合的物理接口称为 slave 接口，聚合后的逻辑 bond 端口称为 master 接口。聚合端口作为逻辑端口，根据添加时输入的 ID 号，bond 接口命名从 bond0—bond3，最多支持 4 个。

说明

- ✧ 一个物理接口只能属于一个 bond 接口。
- ✧ 已经加入到接口联动组中的接口不能再加入到链路聚合中。
- ✧ 支持在 bond 接口上做 GRE（但是反过来不行，GRE 是虚接口，不可以把 GRE 接口加入端口聚合）。

在网络卫士安全网关上设置链路聚合的步骤描述如下：

1) 在管理界面左侧导航菜单中选择 **网络管理 > 接入**，然后选择“链路聚合”页签，如下图所示。



2) 添加新的聚合端口

点击“添加”，添加新的聚合端口，界面如下图所示。

参数说明如下表所示：

参数	说明
ID	选择聚合端口的 ID 号，可选值为 0、1、2、3，bond 接口命名为 bond+ID 号，例如此处设定为 0，则新添加的 bond 端口为 bond0。
负载算法	设置负载均衡算法，将流量分配给聚合链路内不同的物理接口。可选项为： 1) 根据源 mac 地址均衡：表示对发送的报文的源 MAC 地址进行哈希计算，决定将数据分配给聚合端口内哪个 slave 接口。 2) 根据目的 mac 地址均衡：表示对发送的报文的目的 MAC 地址进行哈希

参数	说明
	计算，决定将数据分配给聚合端口内哪个 slave 接口。 3) 根据源和目的 mac 地址组合均衡：表示对发送的报文的源和目的 MAC 地址进行哈希计算，决定将数据分配给聚合端口内哪个 slave 接口。 4) 根据源 IP 地址均衡：表示对发送的报文的源 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 5) 根据目的 IP 地址均衡：表示对发送的报文的目的 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 6) 根据源和目的 IP 地址组合均衡：表示对发送的报文的源和目的 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 7) 根据源 TCP/UDP 端口均衡：表示对发送的报文的源端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 8) 根据目的 TCP/UDP 端口均衡：表示对发送的报文的目的端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 9) 根据源和目的 TCP/UDP 端口组合均衡：表示对发送的报文的源和目的端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 10) 根据五元组均衡：表示根据源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 11) 根据发送端口的轮流均衡：表示发送数据时进行轮询，依次使用从第一个到最后一个可用的 slave 接口。
物理接口	选择将哪些物理接口加入到该聚合端口中。 网络卫士安全网关只支持将工作在路由模式下的物理接口添加到聚合端口中，而且参与聚合的物理接口必须具备相同的速度、MTU、单双工模式属性，而且不能在静态 ARP 表中有相关选项。

参数设置完成后，点击“确定”按钮完成聚合链路添加，新添加的逻辑端口将显示在界面中，如下图所示。

ADSL	虚拟线	链路聚合	802.1x	VLAN-VPN	
+ 添加					总计: 1
名称	负载算法	物理接口	编辑	属性	删除
bond0	根据源mac地址均衡	eth1			

3) 设置聚合端口属性

点击“属性”一列对应的图标可以设置聚合后的端口的接口属性，界面如下图所示。

ADSL
虚拟线
链路聚合
802.1x
VLAN-VPN

聚合端口设置

名称 bond0
 描述
 状态 ☐ 停用
 模式 ☒ 路由 ☐ 交换
 路由模式

地址
 地址

掩码
 掩码

非同步地址 ☐
 属性

地址

掩码

属性

删除

高级 ☐

属性参数解释请参见 [6.2.1物理接口](#)。不同的是，不能设置bond接口的MAC地址、接口速率等参数。加入链路聚合的端口其属性显示为“SLAVE”，如下图所示。

物理接口		子接口							
接口名称	描述	接口模式	地址	MTU	状态	链接	协商	速率	设置
eth0	intranet	路由	192.168.83.233/255.255.255.0	1500	启用		半双工	10M	
eth1	internet	SLAVE		1500	启用				
eth2	ssn	路由		1500	启用				
eth3		交换trunk(3, 103)		1500	启用				

当物理接口加入 bond 成为 slave 接口后，不能对它再进行 IP 层以上的配置，即禁止设置 slave 设备的 ip 地址、MAC 地址、MTU 值、mss-adjust 值、子接口，禁止设置 slave 设备为交换口。只能启用/禁用接口，配置接口 speed、配置 MTU 值。

4) 修改参数

对于已添加的聚合端口，可以点击对应的编辑图标对其参数进行修改。

5) 删除聚合端口

点击对应的删除图标可以删除该户聚合端口。

6.5.4 802.1X 认证

IEEE 802.1x 称为基于端口的访问控制协议，当用户接入网络卫士安全网关设备的路由接口时，如果接口启用了 802.1X 认证，将对接入用户进行 802.1X 认证。合法用户接入时该接口打开，而对于非法用户接入或没有用户接入时，则接口处于关闭状态。

802.1X 认证的相关配置有：

1) 要实现对用户的 802.1X认证，需要管理员在“用户认证”模块添加用户及其所属角色，否则无法认证成功，用户相关设置请参见 [8用户认证](#)。

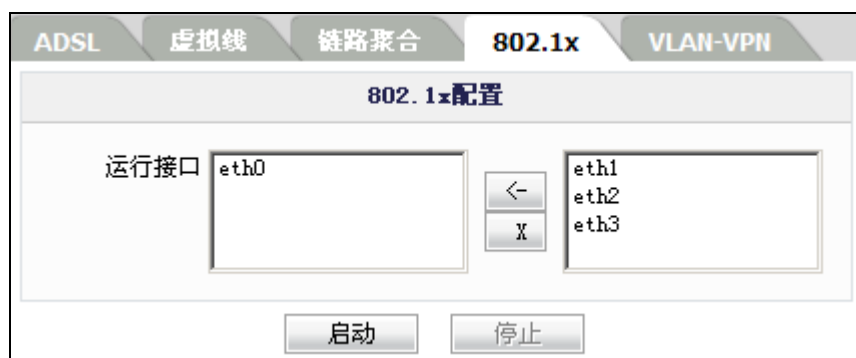
2) 802.1X认证成功之后，对于经过topsec修改的xsupplicant客户端，支持可信接入的检查。如果对该用户或其所属的角色设置了可信接入规则（请参见 [8.5可信接入](#)），还会对客户端进行可信接入规则的检查。对于标准的xsupplicant和windows自带的客户端，不支持可信接入的检查。

说明

- ✧ 只有 x86 系列的网络卫士安全网关产品具有 802.1x 认证的功能，425 平台的设备上不具备此功能。
- ✧ 802.1X 认证方式，目前只支持 md5 挑战字的方式，暂不支持其他认证方式。
- ✧ 网络卫士安全网关支持的 802.1X认证客户端有xsupplicant和windows自带的 802.1x客户端。因为windows自带的客户端是DHCP触发的，所以使用时，需要把windows机器的IP地址设置成“自动获取”，并在安全网关设备上开放DHCP服务。如果使用安全网关作为DHCP服务器，还需要配置相关功能，请参见 [6.6.1安全网关作为DHCP服务器](#)。Xsppllicant客户端没有此限制。

在接口上启用 802.1X 认证的配置步骤描述如下：

1) 选择 **网络管理 > 接入**，并选择“802.1X”页签，进入设定页面，如下图所示。



2) 选择运行 802.1X 认证服务的接口，只能是工作在路由模式的物理接口，不支持 VLAN 虚接口和其他虚拟接口。而且 802.1X 认证服务可以同时运行在多个接口上。

点击“启动”后该接口将对用户启用 802.1X 认证。

3) 点击“停止”即可停止 802.1X 认证。

6.5.5 VLAN-VPN

IEEE802.1Q 定义的 VLAN Tag 域中，只有 12 个比特位用于表示 VLAN ID，所以设备最多可以支持 4094 个 VLAN。但在实际应用中，尤其是在城域网中，需要大量的 VLAN 来隔离用户，4094 个 VLAN 远远不能满足需求。

VLAN-VPN 功能是一种简单、灵活的二层 VPN 技术，通过给报文封装两层 VLAN Tag，即将用户私网的 VLAN Tag 封装在公网的 VLAN Tag 中，从而最多可以提供 4094 × 4094 个 VLAN，满足了城域网对 VLAN 数量的需求。同时，由于用户的私网 VLAN Tag 被公网 VLAN Tag 屏蔽，也可以为用户提供一种较为简单的二层 VPN 隧道。

网络卫士安全网关支持在交换模式的接口上启用 VLAN-VPN 功能。当开启交换接口的 VLAN-VPN 功能后，接口接收到报文时，无论报文是否带有 VLAN Tag，安全网关都会为该报文打上本端口缺省 VLAN 的 VLAN Tag。这样，如果接收到的是已经带有 VLAN Tag 的报文，该报文就成为双 Tag 的报文；如果接收到的是不带 VLAN Tag 的报文，该报文就成为带有端口缺省 VLAN Tag 的报文。

设置步骤为：

1) 选择 **网络管理 > 接入**，并激活“VLAN-VPN”页签，界面如下图所示。

ADSL	虚拟线	链路聚合	802.1x	VLAN-VPN	
+ 添加					总计: 0
接口名称	VLAN ID	模式	协议类型值	删除	

2) 点击“添加”，开启交换接口的 VLAN-VPN 功能，默认不开启。界面如下图。

ADSL

虚拟线

链路聚合

802.1x

VLAN-VPN

VLAN-VPN

接口名称

eth2

模式

access

VLAN ID

1

协议类型值

0x8100

确定

取消

参数说明如下表所示：

参数	说明
接口名称	选择工作在“交换模式”的物理接口名称。
模式	显示该交换接口的工作模式为 access 或 trunk。
VLAN ID	显示该交换接口所属 VLAN 的 ID 号。
协议类型值	VLAN-VPN 的协议类型由报文外层 VLAN Tag 中的 TPID 字段来标识，不同厂商的设备只有具有相同的 TPID 值才能实现互通。网络卫士安全网关支持 TPID 调整功能，可以与 TPID 为 0x8100 和 0x9100 的厂商的设备实现互通。 默认为 0x8100。

点击“确定”完成 VLAN-VPN 设置。

3) 点击“删除”一栏的删除图标，可以删除接口的 VLAN-VPN 功能设置。

6.6 DHCP

DHCP（动态主机配置协议）是 Dynamic Host Configuration Protocol 的缩写，DHCP 的目的是为网络中的主机自动进行 IP 地址分配及其他 IP 相关设置。通过 DHCP，可以简化网络管理员的工作，实现 IP 地址集中、高效的管理。

DHCP 服务工作在典型的 Client/Server 方式下。DHCP 服务器负责集中管理和维护 IP 配置信息，处理客户机的 DHCP 请求并进行 IP 地址的动态分配和租期管理，同时还可以向客户机提供其他的 IP 配置信息，如默认网关、DNS 及 WINS 服务器的 IP 地址等等。DHCP 客户机则会使用分配的 IP 及其他信息进行 IP 环境配置。如果 DHCP 服务器和 DHCP 客户机不在同一子网内（一个广播域），则需要路由设备支持 DHCP 报文的转发（DHCP 中继）。

网络卫士安全网关提供比较全面的 DHCP 服务功能，能够很好地结合到客户网络环境中。网络卫士安全网关可以提供以下 DHCP 服务：

- 作为 DHCP 客户端，从 DHCP 服务器获取动态 IP 地址。
- 作为 DHCP 服务器，集中管理和维护客户网络主机 IP 地址分配。
- 作为 DHCP 中继，转发 DHCP 报文。
- 同时作为 DHCP 服务器和 DHCP 客户机（需工作在网络卫士安全网关的不同接口上）。

说明

- ✧ 如果需要使用安全网关的 DHCP 功能，需要开放 DHCP 服务，具体请参见 [4.2.2.2 开放服务](#)。

6.6.1 安全网关作为 DHCP 服务器

网络卫士安全网关可以指定某个物理接口、VLAN 虚接口、lo 接口和聚合端口作为 DHCP 服务器，为该接口所在子网的主机动态分配 IP 地址，此时该接口必须工作在路由模式下。

配置安全网关作为 DHCP 服务器，需要首先配置地址池，才能在相应接口运行 DHCP 服务器。还需要在相应的接口开放 DHCP 服务，否则不能提供 DHCP Server 的服务，具体请参见 [4.2.2.2 开放服务](#)。

具体设置参数的方法如下：

1) 在左侧导航菜单中选择 **网络管理 > DHCP**，点击“DHCP 服务器”页签，如下图所示。

DHCP服务器
DHCP客户端
DHCP中继

DHCP服务

运行接口

<-

X

eth0
eth1
eth2
eth3

启动

停止

查看分配地址

地址池 + 添加地址池

作用域	地址范围	缺省租用期	最大租用期	选项	删除
11.11.11.0 /255.255.255.0	11.11.11.10- 11.11.11.60	1天-0小时-0分钟	7天-0小时-0分钟		

地址绑定 + 添加地址绑定

名称	IP地址	物理地址	删除

2) 设置地址池。

当 DHCP 服务器处于“运行”状态时，“添加地址池”按钮不可见，地址池中每一个项目的删除图标显示为“—”，不可进行删除操作。

a) 添加地址池

当 DHCP 服务器处于“停止”状态时，点击“添加地址池”，设置网络卫士安全网关可分配的地址池的相关参数。如下图所示。

添加DHCP地址池

子网 *

掩码 *

分配起始地址 *

分配结束地址 *

缺省租用期 天 时 分

最大租用期 天 时 分

网关地址

主DNS

次DNS

域名

客户端类型

供应商详情

确定

取消

参数说明如下表所示。

参数	说明
子网/掩码	设置为哪个子网创建 DHCP 作用域。
分配起始地址/分配结束地址	输入 DHCP 服务器可以为客户端分配地址的范围。应当与“子网”设定的 IP 在同一个网段，并且不能包含已经分配的 IP 地址。
缺省租用期	DHCP 服务器向 DHCP 客户端租借地址的期限。到期后如果客户端要继续使用该地址则必须续订。默认为 1 天。 说明： 缺省租用期一定不能高于最大租用期。
最大租用期	服务器端为客户保留地址的最长时期。这个宽限期在出现以下情况时保护客户端租约：客户端和服务端处于不同的时区、个别计算机的时钟没有同步、在租约过期时客户端从网络上断开。默认为 7 天。 说明： 缺省租用期一定不能高于最大租用期。
网关地址	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定其网关地址。
主 DNS/次 DNS	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定主/次 DNS 服务器地址。
域名	可选项，为网络上的客户计算机用来进行 DNS 名称解析时使用的父域。
客户端类型	可选项，用于配置用户定义类别，从而为 DHCP 客户端定义用户类别。当 DHCP 客户端向 DHCP 服务器请求 IP 租约时，DHCP 服务器可以识别这种用户类别，并可以根据用户类别配置 DHCP 选项。 例如一个网络教室里的教师用计算机和学生用计算机需要各自专用的网关，通过网关的设置来限定对某些资源的访问使用，则可以定义两个用户类别：STUDENT 和 TEACHER，然后在客户端设置使用这两个用户类别，既可以做到教师用计算机和学生用计算机具有不同网关，从而可以限制学生用计算机对某些资源的访问。
供应商详情	可选项，用于配置供应商类别：DHCP 服务器可以自动识别运行某些操作系统的计算机所发送的特定的标识符，例如 DHCP 服务器可以识别 DHCP 客户端运行的操作系统是否是 Windows2000 或 Windows98 等。通过对标识符的识别，可以将 DHCP 选项分配给基于特定操作系统的 DHCP 客户端。

设置完成后，点击“确定”按钮。界面会显示已经添加的地址池项目。

b) 删除地址池

选择一个或多个地址池，或直接点击“全选”按钮选择所有地址池，然后点击“删除”按钮可以删除地址池。

3) 设置地址绑定，管理员可以在租约期内保留一个特定的 IP 地址供某台 DHCP 客户端主机（由 MAC 地址来标识）使用。

地址绑定	 添加地址绑定		
	名称	IP地址	物理地址
			删除

a) 添加地址绑定

当 DHCP 服务器处于“运行”状态时，“添加地址绑定”按钮不可见。当 DHCP 服务器处于“停止”状态时，在“DHCP 服务器”页面点击“添加地址绑定”，如下图所示。

参数说明如下表所示。

参数	说明
名称	添加该地址绑定规则的名称。
主机地址	需要绑定的 IP 地址，绑定的 IP 地址可以是地址池的可分配 IP 范围之内，也可以是可分配 IP 范围之外，但必须在在添加地址池时指定的 DHCP 服务器的作用域之内。
物理地址	主机的 MAC 地址，16 进制字母大小写输入均可。

设置完成后，点击“确定”按钮，如果添加成功，则界面中会显示已经添加的地址绑定项目，如下图所示。

地址绑定 + 添加地址绑定			
名称	IP地址	物理地址	删除
bind	100.1.1.1	00:09:10:23:32:34	

b) 删除地址绑定

选择一个或多个地址绑定，或直接点击“全选”按钮选择所有地址绑定，然后点击“删除”按钮可以删除地址绑定。

4) 若要删除某 DHCP 服务条目，点击该条目所在行的删除图标进行删除。

5) 启动 DHCP 服务器进程

a) 在页面左上方“运行接口”处设置提供 DHCP 服务的物理接口、VLAN 虚接口名、lo 接口以及聚合端口。当选择物理接口或 VLAN 虚接口时，网络卫士安全网关可为此接口区域内的主机动态分配 IP 地址。当选择 lo 时，用于为 SSL VPN 模块的全网接入功能分配地址。

The screenshot shows the 'DHCP 服务' (DHCP Service) configuration window. It has a title bar with the text 'DHCP 服务'. Inside, there is a section labeled '运行接口' (Running Interface) with an empty text box. To the right of this box are two buttons: '<' and 'X'. Further right is a list box containing the interface names 'eth0', 'eth1', 'eth2', and 'eth3'. At the bottom of the window are three buttons: '启动' (Start), '停止' (Stop), and '查看分配地址' (View Assigned Address).

DHCP SERVER 服务可以同时运行在多个接口上，如下图所示。

The screenshot shows the 'DHCP 服务' (DHCP Service) configuration window with multiple interfaces selected. The '运行接口' (Running Interface) text box now contains 'eth0' and 'eth2'. The list box on the right contains 'eth1', 'eth3', 'sslvpn0', and 'vlan.0001'. The buttons at the bottom are '启动' (Start), '停止' (Stop), and '查看分配地址' (View Assigned Address).

b) 其他参数设置完成后，点击“启动”即可在该接口启动 DHCP 服务。

说明

- ✧ 只有在添加了 DHCP 地址池后才能够除了在除了 lo 以外的其余接口启动 DHCP 服务。在 lo 接口上启动 DHCP 服务无需设置地址池。

7) 点击“查看分配地址”，可以在已分配地址栏显示安全网关作为 DHCP 服务器为客户端动态分配的 IP 地址。

已分配地址			
			总计: 1
IP	MAC	租约开始	租约结束
10.10.10.20	00:50:04:e3:b0:31	2009/09/07 16:46:32	2009/09/08 16:46:32

6.6.2 安全网关作为 DHCP 客户端

网络卫士安全网关作为 DHCP 客户端，接口可以自动获取 IP 地址。在这种情况下，网络卫士安全网关的指定接口将由 DHCP 服务器动态分配 IP 地址。

说明

- ◇ DHCP Client 服务可以同时运行在多个接口上。
- ◇ 安全网关接口作为 DHCP 客户端时所连接的 DHCP 服务器不能与别的物理接口或 VLAN 虚接口处于同一个网段，否则即使此处运行成功也不能正确获取 IP。
- ◇ 还需要在安全网关作为客户端的接口向 DHCP 服务器开放 DHCP 服务。具体请参见 [4.2.2.2 开放服务](#)。

配置方法如下：

1) 在左侧导航菜单中选择 **网络管理 > DHCP**，点击“DHCP客户端”页签，如下图所示。



2) 设置要自动获得 IP 地址的接口，可以是物理接口、VLAN 虚接口、聚合端口和 lo 口。

DHCP 客户端服务可以同时运行在多个接口上，如下图所示。



点击“启动”后该接口将从 DHCP 服务器自动获取 IP 地址。

3) 要禁止接口获得 IP 地址，点击“停止”，该接口将停止从 DHCP 服务器自动获取 IP 地址。

6.6.3 安全网关作为 DHCP 中继

当 DHCP 客户端和 DHCP 服务器不在同一个网段时，客户端和服务端中间必须有 DHCP 中继代理将它连接的其中一个物理接口（如网卡）上广播的 DHCP/BOOTP 消息中转到其他物理接口连至的其他远程子网。

网络卫士安全网关可以作为 DHCP 中继代理，帮助客户机从其他网段的 DHCP 服务器获取 IP 地址及其他配置参数，如默认网关、DNS 等等。管理员还需要在安全网关上开放服务器和客户机所属区域的 DHCP 服务。具体请参见[4.2.2.2 开放服务](#)。

具体设置方法为：

1) 在左侧导航菜单中选择 **网络管理 > DHCP**，点击“DHCP 中继”页签，如下图所示。

The screenshot shows the 'DHCP中继' (DHCP Relay) configuration window. It features a '配置' (Configuration) section with two main input areas. The first, '指定接口' (Specify Interface), includes a list box with options 'eth0', 'eth1', 'eth2', and 'eth3'. The second, '服务器地址' (Server Address), includes a text input field. Both areas have '<' and 'X' buttons. At the bottom, there are '启动' (Start) and '停止' (Stop) buttons.

2) 在“指定接口”处选择与 DHCP 客户端相连的安全网关接口，同时还要选择与 DHCP Server 相连的安全网关接口，如下图所示。



3) 点击“启动”，启动中继服务。

说明

- ◇ DHCP 中继服务可以同时运行在多个接口上。
- ◇ 如果 DHCP 服务器的默认网关不是安全网关的接口（虚接口）地址，必须在该服务器上添加一条静态路由，目的地址为 DHCP 服务器作用域的网段，网关地址为安全网关与 DHCP 服务器连接的接口地址，否则客户机无法正确获取 IP。

6.7 流量管理

网络卫士安全网关通过配置 QoS 策略实现网络带宽的动态管理。还可以根据物理接口、地址对象、常用端口和 IP 连接信息对通过设备的流量信息进行统计。

6.7.1 QoS

网络卫士安全网关支持网络带宽的动态管理,通过在访问控制规则中引用提前配置的 QoS策略，或者直接在访问控制规则中设置QoS策略，可以基于网络连接的源IP地址、目的IP地址、协议、服务、时间段，对数据流设置细粒度的带宽管理策略。访问控制规则设置请参见 [9.2.5添加规则](#)。在QoS策略中可以设置数据流量需要保证的最小平均带宽（即保证带宽）和可以获得的最大带宽（即限制带宽）。对于同一个连接，还可以对数据传输的上行和下行两个方向设置不同的带宽管理策略，“上行”和“下行”都是相对ACL策略的源IP而言，源IP上传数据时称“上行”，下载数据则称“下行”。

策略分为 4 种：共享、独享、受控和策略独享。

➤ 共享类

当多个访问控制规则引用同一个 QoS 策略时，所有匹配 ACL 规则的连接共享 QoS 中设置的保证带宽和限制带宽。

➤ 策略独享类

当多个访问控制规则引用同一个 QoS 策略时，每一个 ACL 规则中匹配的所有连接各自共享 QoS 中设置的保证带宽和限制带宽。

➤ 独享类

匹配 ACL 策略的每一个连接都单独享有 QoS 中设置的保证带宽和限制带宽，并且不对总的带宽加以限制。

➤ 受控独享类

匹配 ACL 策略的每一个连接都单独享有 QoS 中设置的“每主机限制带宽”，但是所有源 IP 可以使用的总带宽不能超过 QoS 设定的“总限制带宽”。

管理员可以在此直接添加 QoS 策略，也可以直接在访问控制规则中设置 QoS 参数。

说明

- ◇ 如果用户需要保证某个连接的传输带宽，则还必须进行如下相关设置：（1）配置转发接口的有效带宽。（2）在 ACL 策略中必须设置“源区域”或“目的区域”参数（对于上行数据需设置“目的区域”，对于下行数据则需设置“源区域”），而且“源区域”或“目的区域”下所有的保证带宽之和不能超过接口的有效带宽。

设置 QoS 策略的步骤为：

- 1) 选择 **网络管理 > 流量管理**，激活“QoS”页签，如下图所示。

名称	上行	下行	操作
ftp_up		类型：策略独享 保证带宽：10KBps 限制带宽：12KBps 优先级：中	

接口名称	带宽	操作

“QoS 策略”下方的列表框中显示管理员手工添加的 QoS 策略。

- 2) 设置 QoS 策略：

策略设置包括添加、修改和删除三种。

a) 添加 QoS 策略

点击“添加”，添加“带宽限制”策略，当策略类型选择“共享”以外的其他类型时，上行和下行可以设置不同类型的控制策略。

当策略类型选择“共享”、“策略独享”和“独享”时参数如下图蓝色框内所示；当策略类型选择“受控”时参数如下图红色框内所示。

参数说明如下表所示：

参数	说明
策略名称	输入策略的名称。在对象下方选择 QoS 策略的类型，可选项为共享、独享、受控和策略独享。
优先级	设置该策略的优先级。可选项为“特权”、“高”、“中”和“低”4 级优先级。“特权”为最高优先级。在网络拥塞的情况下，QoS 策略的优先级高，与引用该 QoS 策略的 ACL 规则匹配的数据流就能够优先享有带宽服务。 说明： 只有“保证带宽”或“限制带宽”中至少一项设置数值之后，该选项才为可选择状态。
总带宽限制	当“策略类型”选择“受控”时需要设置该项。设置当数据流匹配引用该对象的 ACL 策略时，所有匹配该规则的 IP 地址的总的限制带宽。
每主机限制带宽	当“策略类型”选择“受控”时，需要设置该项。设置当数据流匹配引用该对象的 ACL 策略时，匹配该规则的每一个 IP 地址都单独享有限制带宽。
保证带宽	当“策略类型”选择“共享”、“策略独享”和“独享”时需要设置该项。设置当数据流匹配引用该对象的 ACL 策略时，在传输过程中能够保证的最小平均带宽。 说明： 要保证某些连接的传输带宽，必须进行如下相关设置： 1) 必须设置数据流的出接口的有效带宽，即QoS中设置“上行”保证带宽，则必须设置“目的接口”的有效带宽；设置“下行”的保证带宽则必须设

参数	说明
	置“源接口”的有效带宽。而且，接口设定的有效带宽值必须要大于所有同一接口区域范围内所有访问控制中保证类带宽的和；具体说明请参见 设置接口的有效带宽 。 2) 必须在引用 QoS 对象的 ACL 规则中设置数据出接口的区域，即 QoS 中设置“上行”策略时，引用该 QoS 的 ACL 中必须设置“目的区域”；QoS 中设置“下行”策略时，引用该 QoS 的 ACL 中必须设置“源区域”。 3) 区域对象中只能包含一个接口属性。具体设置请参见 7.2设置区域资源 。
限制带宽	当“策略类型”选择“共享”、“策略独享”和“独享”时需要设置该项。设置当数据流匹配引用该对象的 ACL 策略时，在传输过程中可获得的最大带宽。

点击“确定”完成对象添加。

b) 修改策略属性

对于已经添加的策略，可以点击“修改”图标对其参数进行修改。只能修改上行（下行）保证带宽、上行（下行）限制带宽、上行（下行）优先级。

c) 删除策略

如果策略未被 ACL 规则引用，则点击“删除”图标可以将某策略删除。

3) 设置接口的有效带宽

如果在 QoS 策略中设置了保证带宽，并在 ACL 规则中引用了该类 QoS 策略，则必须设置出接口的有效带宽，否则 ACL 中无法引用该类 QoS 策略。如果所有同一接口区域范围内访问控制中引用的所有 QoS 对象均只设置了限制带宽，则不需要配置接口的有效带宽。

设置界面如下图所示。

接口有效带宽		
+ 添加		
接口名称	带宽	操作

a) 点击“添加”，设置接口的有效带宽，界面如下图。

接口带宽

接口名称

eth0

带宽

0

Kbps

确定

取消

参数说明如下表所示：

参数	说明
接口名称	在下拉列表中选择接口名称，可以是物理接口、子接口、聚合端口或 IPSec 虚接口，不能是 VLAN 虚接口和 PPPoE 接口的名称。
带宽	输入该接口的总的出口带宽和单位。 说明： 接口带宽值要大于所有同一接口区域范围内访问控制中保证类带宽之和。 例如：如果在接口上有 m 个 ACL 引用“共享”类 QoS（保证带宽为 X），n 个 ACL 引用“策略独享”类 QoS（保证带宽为 Y），p 个 ACL（共有 q 个可能匹配的连接）引用“独享”类 QoS（保证带宽为 Z）。由于“共享”类的所有源 IP 共享保证带宽；“策略独享”类的每个 ACL 策略都分别占用保证带宽，“独享”类的每个源 IP 都各自独享保证带宽，因此接口有效带宽值必须设置大于 $(X+n*Y+q*Z)$ 的数值。

点击“确定”即可。

b) 修改出口带宽设置

点击“修改”图标即可修改设置。

c) 删除出口带宽设置

点击“删除”图标即可删除设置。

6.7.2 地址统计

网络卫士安全网关支持对通过安全网关的数据报文的流量进行统计的功能。根据地址对象进行数据流量信息，包括主机地址对象、子网地址对象、范围地址对象等，并支持查看特定地址对象的具体流量信息、对流量进行排序以及查看流量为 TOPN 的地址对象等功能。

1) 选择 **网络管理 > 流量管理**，激活“地址统计”页签，可以根据 IP 地址查看其流量信息，如下图所示。

2) 点击“流量开关”右侧的“开启”按钮，可以启动安全网关对地址资源进行流量统计的功能。

3) 设置需要统计流量的资源

点击“添加地址”，可以选择需要进行流量统计的地址资源，界面如下图所示。



地址资源添加完成后，点击“确定”，则添加的资源会显示在列表中，如下图所示。



4) 查看流量统计信息

a) 在上图中，点击指定地址对象左侧的“▶”图标，可以查看与此地址资源相关的流量统计信息，如下图所示。



如果点击“地址对象名称”字段左侧的三角图标，则将列表中所有的地址资源的流量统计情况同时列表显示，如下图所示。

统计结果

刷新

+ 添加地址

IP地址:

查找

前N个IP的流量:

显示

▼地址对象名称

删除

▼192.168.83.226

▼192.168.83.224

IP地址	TCP			UDP			ICMP			总流量(字节)
	入字节	出字节	包数	入字节	出字节	包数	入字节	出字节	包数	
192.168.83.224	61759	46450	665	0	3500	41	0	0	0	111709

▼192.168.83.220

IP地址	TCP			UDP			ICMP			总流量(字节)
	入字节	出字节	包数	入字节	出字节	包数	入字节	出字节	包数	
192.168.83.220	10848	3000	301	67350	13876	317	924	14124	97	110122

b) 点击指定地址资源对应的“删除”图标，可以删除该地址资源，此时将停止对其进行流量统计。

c) 点击“刷新”按钮或点击 WEB 页面右上角的“刷新页面”，可以更新流量统计信息。

d) 点击“停止”按钮，则列表中的所有地址对象的流量统计信息均被删除。

5) 查找指定的地址资源

在“IP 地址”右侧的文本框中输入 IP 地址，点击“查找”按钮，可以查询已经添加到地址统计对象中的地址资源。

IP 地址的查找遵循从上到下顺序匹配的原则，界面的查询结果只显示第一个匹配的地址资源。例如，当在“IP 地址”处输入 192.168.83.234 时，点击“查找”，则结果如下图所示。

统计结果

 刷新  添加地址

IP地址: 192.168.83.224  前N个IP的流量:  显示

▶ 地址对象名称

▶ doc 

删除

说明

- ✧ 如果在将地址资源设置为统计对象之后，管理员又对地址资源进行了修改，则需要管理员重新设置统计对象，否则地址资源的变更在这里无法体现。

6) 查看前 N 位的统计信息

在“前 N 个 IP 的流量”右侧的文本框中输入数值 N（N 的取值范围为 1-1000），并点击“显示”后，可以查看已经启动流量统计的总流量为前 N 位的地址资源流量统计结果。如下图所示。

统计结果

刷新 + 添加地址

IP地址: 查找 前N个IP的流量: 1 显示

IP地址	TCP			UDP			ICMP			总流量
	接收字节	发送字节	包数	接收字节	发送字节	包数	接收字节	发送字节	包数	
192.168.83.224	218069	48210	698	0	2179	26	0	0	0	268458

6.7.3 常用端口流量统计

网络卫士安全网关可以对连接中所有的 IP 地址（源 IP 和目的 IP）在各个端口上的流量进行分别统计，统计项目包括发送和接收的流量、新建连接数和在所有端口的总流量。总流量只统计发送、接收的字节数，不统计连接数。

默认情况下系统只对连接中的所有 IP 在 80、8080、20、21、110、25 这 6 个固定端口上的流量进行分别统计，管理员可以根据实际情况设置对其他端口进行流量统计，但是一次只能统计 6 个端口的流量信息。

每一个 IP 地址的端口流量统计信息为一项，如果管理员正确设置了日志服务器的相关选项（包括 IP 地址、设置传输选项，并选择“端口流量”日志类型），端口流量的统计信息将发送给日志服务器，安全网关将以“项”为单位向日志服务器发送流量统计信息，当有多项时，将按照设定的发送时间间隔分项进行发送。

1) 选择 **网络管理 > 流量管理**，激活“端口统计”页签，如下图所示。

QOS 地址统计 端口统计 IP连接统计

参数设置

统计时间间隔: [范围: 300-86400s]

发送时间间隔: [范围: 1-10s]

端口: 1: 2: 3: 4: 5: 6:

统计结果

显示: 来源 ▼ IP地址: 查找

刷新

IP	端口	发送字节	接收字节	新建连接数	连接时间

2) 在“参数设置”处，管理员可以修改系统默认的统计参数。

参数说明如下表所示：

参数	说明
统计时间间隔	设置流量统计的时间间隔。默认为 1800 秒（半小时），范围为 300—86400 秒。
发送时间间隔	设置发送统计数据的时间间隔。默认为 1s。范围为 1—10 秒。 说明： 统计数据以日志的形式发送出去，因此管理员还需通过 日志与报警>日志设置 选择“端口流量”的日志类型。
端口	设置要统计流量的端口信息。 网络卫士安全网关最多只支持同时统计 6 个端口的数据，默认情况下统计 80、8080、20、21、110、25 这 6 个固定端口的流量。管理员可以根据需求进行修改，修改完成后点击“确定”按钮即可立即生效。 说明： 如果一个 IP 在修改端口之前存在统计表项，修改端口后的会立即删除原来的统计项、建立新的统计表项。

点击“确认”完成参数修改。

3) 点击“开启”按钮，开启安全网关的端口流量统计功能。

开启后，管理员点击“停止”，将关闭安全网关的端口流量统计功能。

4) 查看统计结果

a) 在“统计结果”处显示统计结果。默认只显示连接中源 IP 的端口流量信息，如下图所示。

统计结果

显示

来源

IP地址

查找

刷新

IP	端口	发送字节	接收字节	新建连接数	连接时间
192.168.83.224	80	0	0	0	Wed Jun 23 07:08:29 2010
	8080	3653	21290	4	
	20	0	0	0	
	21	0	0	0	
	110	0	0	0	
	25	0	0	0	
	总计	3653	21290		
192.168.83.226	80	0	0	0	Wed Jun 23 07:08:44 2010
	8080	1788	13733	1	
	20	0	0	0	
	21	0	0	0	
	110	0	0	0	
	25	0	0	0	
	总计	1788	13733		

在“显示”一栏选择“目的”，将只显示通过安全网关的连接中目的 IP 的端口流量信息。

b) 点击“刷新”按钮可以得到最新的流量统计信息。

c) 查找指定 IP 地址的端口流量统计信息

在“IP 地址”处输入查找的 IP 地址，点击“查找”按钮，则符合条件的流量信息将显示在下面的统计结果列表中。如下图所示。

统计结果					
显示	来源	IP地址	192.168.83.224	查找	
刷新					
IP	端口	发送字节	接收字节	新建连接数	连接时间
192.168.83.224	80	0	0	0	Wed Jun 23 07:08:29 2010
	8080	4935	31163	5	
	20	0	0	0	
	21	0	0	0	
	110	0	0	0	
	25	0	0	0	
	总计	4935	31163		

6.7.4 IP 连接统计

网络卫士安全网关支持根据 IP 地址统计 session 个数，即统计流经设备的 IP 报文的源 IP 地址创建的 session 个数信息，包括历史创建 session 总数和最近 n 秒（n 可以设置，范围为 2—30 秒）创建 session 个数，最多可记录 8192 项。通过 IP 连接统计，便于管理员查看当前在线连接数、历史创建连接数和最近 n 秒创建连接数的前 5 名的信息。如果 1 秒钟之内有超过 8192 个 IP 地址新建连接，网络卫士安全网关会向日志服务器发出可能存在源地址欺骗的告警信息；如果 n 秒钟之内某一个 IP 地址的新建连接数超过 1000，也会向日志服务器发送告警信息。

1) 选择 **网络管理 > 流量管理**，并激活“IP连接统计”页签，界面如下图所示。

QoS	地址统计	端口统计	IP连接统计
IP连接统计			
统计开关: 开启 停止			
IP连接数统计间隔时间设置: [2-30s] 应用			
统计结果(前5名)			
刷新			
连接	IP地址	连接数	

2) 在“IP 连接数统计间隔时间设置”处设置连接计数的时间间隔，范围 2—30 秒，默认值为 5 秒。管理员可以修改该数值，修改后需要点击“应用”按钮使修改生效。

3) 点击“开启”按钮启动 IP 连接统计。

4) 查看统计结果

a) 在页面下方的统计结果处将显示 IP 连接的统计信息，如下图所示。

统计结果(前5名)		
 刷新		
连接	IP地址	连接数
在线连接数	192.168.83.224	3
过去5秒建立连接数	192.168.83.224	3
	192.168.83.220	1
建立连接总数	192.168.83.224	3
	192.168.83.220	1

b) 点击“刷新”按钮可以得到最新的 IP 连接统计信息。

6.8 IP 探测

IP 探测通过每隔一定时间向预先设定的 IP 发送 ping 包，来检测链路的状况，并将检测结果在设备上记录。在链路备份、双机热备、静态路由模块中可以引用探测 ID 号，根据 IP 探测的结果作为某条链路是否可用的依据。

说明

- ✧ 只有命令行下利用 **#network route ip-probe on** 命令开启“路由IP探测”，静态路由模块才根据IP探测的结果作为路由是否可用的依据；
- ✧ 双机热备中执行 **#ha ip-probe enable** 后，才根据IP探测的结果作为主从机切换的依据。

具体设置方法为：

1) 选择 **网络管理 > IP探测**，进入参数设定页面，如下图所示。

IP探测							
 添加  清空							
ID	接口	探测IP	探测时间间隔	状态	引用模块	修改	删除
100	eth0	192.168.83.224	5	初始状态			
101	eth1	192.168.83.233	5	初始状态			

“状态”一栏显示当前该链路是否被引用、是否可用。每个探测条目只有被引用的时候才进行探测，否则不进行探测，并且设置状态为“初始状态”。探测通过发送 ping 包进行，当发送的 ping 包有回应时，表明链路状态正常，状态显示为“链路良好”；否则显示为“链路不可达”。

“引用模块”显示引用该链路的模块名称。可以在静态路由模块、链路备份模块和双机热备模块引用探测链路。

2) 添加新的探测链路

点击“添加”，添加新的探测链路，一共可以添加 5 条探测链路。如下图。



IP探测设置

接口: -选择接口- *

探测IP: *

探测时间间隔: 5 [1-3600秒]

确定 取消

参数说明如下表所示：

参数	说明
接口	选择探测的设备出口。可以是物理接口、VLAN 虚接口、bond 口、子接口、ppp0 虚接口等。 说明： 当探测链路在 HA 中引用时，安全网关上用于 IP 探测的接口地址必须配置一个区别于当前通信 IP 的、单独配置的一个“非同步地址” IP，否则这个接口相关的路由会因为安全网关变为从状态而 down 掉。
探测 IP	设置一个链路外部信任的 IP 地址，通过设定的网络接口定时向该主机发送 ping 包来探测链路通讯是否正常。 说明：探测 IP 必须是在正常状态下能够探测到的 IP 地址。
探测时间间隔	设置发送 ping 报文的时间间隔。范围为 1 到 3600。默认为 5。单位为秒。 说明： 探测时间间隔为上次探测结束的时间和下一次探测开始之间的时间间隔。

点击“确定”完成链路添加。新添加的探测条目没有被引用，所以不进行探测，状态显示为“初始状态”。

3) 修改属性

点击某条目对应的修改图标可以修改其属性。如果该条目被其他模块引用，则只能修改其“探测 IP”和“探测时间间隔”。如果没有被引用，则可以修改除了 ID 以外的其他属性。

4) 删除条目

如果某个条目在被其他模块引用，则删除一栏显示为“—”，不允许删除该条目。

点击“删除”图标可以删除该条目。点击“清空”则可以一次性删除所有未被引用的 IP 探测条目。

6.9 域名解析

DNS（Domain Name Server），域名服务器，实现域名地址与 IP 地址的映射，并保证主机域名地址在因特网中唯一。网络卫士安全网关提供了 DNS 服务器的设定功能。也可以不设置 DNS 服务器，此时将采用系统中默认的 DNS 服务器地址，具体地址和匹配的先后顺序为：219.141.140.10、202.96.134.133、202.96.199.132、202.96.0.133、202.96.128.143。

DNS 服务器的具体设置方法如下：

1) 选择 **网络管理 > 域名解析**，进入 DNS 服务器设定页面，如下图所示。

2) 界面中的参数说明如下表：

参数	说明
首选 DNS 服务器	在“首选 DNS 服务器”文本框中输入优先级最高的 DNS 服务器的 IP 地址；如果有备用的 DNS 服务器，则可在“次选 DNS 服务器”文本框中输入其 IP 地址。
测试域名	用于测试 DNS 服务器是否正常。 填写域名后，点击“确定”按钮便可开启 DNS 服务器的探测功能。当 DNS 服务器可用时，右侧会显示绿色图标，不可用时则显示红色图标。
DNS 中继	开启该功能后，网络卫士安全网关便可作为 DNS 服务器使用。此时，安全网关会将 DNS 查询数据重新转发到“首选 DNS 服务器”和“次选 DNS 服务器”。

3) 点击“确定”按钮，使设置生效；点击“清除设置”则删除当前界面中设置的所有信息。

7 资源管理

网络卫士安全网关大多数的功能配置都是基于资源的。如访问控制策略、地址转换策略、服务器负载均衡策略、认证管理等。可以说，定义各种类型的资源是管理员在对网络卫士安全网关进行配置前首先要做的工作之一。

资源概念的使用大大简化了管理员对网络卫士安全网关的管理工作。当某个资源发生变化时，管理员只需要修改资源本身的属性即可，而无需逐一地修改所有涉及到这个资源的策略或规则。

在网络卫士安全网关中，用户可定义的资源类型包括：

- 地址资源：包括主机资源、地址范围资源、子网资源和地址组。
- 区域资源：通过与属性资源绑定，定义区域的访问权限。
- 时间资源：包括多次循环的时间资源和单次时间资源。
- 服务资源：包括系统定义的服务资源、自定义的服务资源和服务组。
- DNS 对象：介绍设置 DNS 关键字对象。

说明

- ◇ 资源名称不允许出现的特殊字符：空格、“'”、“””、“\”、“;”、“'”、“\$”、“&”、“@”、“%”、“|”、“~”、“<”、“>”、“#”、“+”、“!”、“=”、“^”、“?”、“`”。
- ◇ 网络卫士安全网关支持对资源进行重命名操作。
- ◇ 对资源对象进行修改时，如果资源对象被访问控制规则引用，则修改对象后进行保存时系统会进行策略冲突检查，如果对资源对象的修改导致和已有策略冲突，则将拒绝相应修改。

7.1 设置地址资源

地址资源的设置是资源管理中最基本的操作，在定义访问控制规则和地址转换规则时需要选择不同的地址资源，用户可以设置各种类型的地址资源，如主机资源、地址范围资源、子网资源，同时可以定义地址组将这些不同的地址资源添加到地址组中。

各种地址资源及地址组的设置操作请参见下面章节。

将鼠标置于地址资源的名称处，可以查看引用该资源的所有策略。

7.1.1 设置主机资源

1) 选择 **资源管理** > **地址**，并在右侧页面中选择“主机”页签，将会显示已有的主机资源，如下图所示。

主机		范围	子网	地址组
+ 添加		清空		总计: 9
名称	IP地址	操作		
server1	192.168.83.2			
host1	192.168.83.56			
server2	192.168.83.2			
WebServer1	192.168.83.234			
WebServer2	192.168.83.235			
WebServer	10.1.1.10			
doc	192.168.83.224			
192.168.83.234	192.168.83.234			
1				

上图中，“删除”一列为“—”表示该主机资源对象被规则引用，无法删除。

将鼠标置于对象名称处，可以查看引用该对象的所有策略，如下图所示。

主机			范围	子网	地址组
+ 添加			清空		
					总计: 13
名称	IP地址	操作			
webserver		NAT-POLICY 8092			
202.99.1.3	202.99.1.3				
202.98.1.3	202.98.1.3				
172.16.98.222	172.16.98.222				
DHCP Server	192.168.83.234				

2) 添加主机资源

点击“添加”，系统出现添加主机属性的页面，如下图所示。

页面中各参数的含义如下。

参数	说明
名称	用户定义的主机资源的名称。
物理地址	主机的MAC地址。当用户同时设置了主机的MAC地址和IP地址时，添加主机后，也会增加一条IP/MAC地址绑定策略。用户可以通过 防火墙 > IP/MAC绑定 进行查看。
IP 地址	设置该主机资源的 IP 地址应满足的约束条件。 在右侧的文本框中输入 IP 地址字符串，点击“←”按钮，则出现在左侧的文本框中。 说明： 可以对同一个主机资源输入多个 IP 地址，则只要满足其中一个条件即可。最多可以输入 120 个 IP 地址，以方便对多 IP 用户的控制。

点击“确定”完成主机资源的设定。

3) 修改资源属性

点击对应的“修改”图标可以修改已设定的主机资源。

4) 删除资源

如果主机资源对应的“删除”一列为图标“”，则表明该主机资源未被引用，点击“删除”图标可以删除该资源。如果主机资源对应的“删除”一列为图标“—”，则表明该主机资源被引用，无法删除。

点击“清空”可以清除所有**未被引用**的主机资源。

7.1.2 设置地址范围资源

1) 选择 **资源管理 > 地址**，选择“范围”页签，右侧界面显示已有的地址范围资源，如下图所示。

主机	范围	子网	地址组
+ 添加 清除 总计: 3			
名称	起始地址	终止地址	排除地址
any	0.0.0.0	255.255.255.255	
rdm	192.168.84.0	192.168.84.225	
rddoc	192.168.83.220	192.168.83.228	

上图中，“删除”一列为“—”表示该资源对象被规则引用，无法删除。

2) 添加资源

点击“添加”，进入地址范围属性的页面，如下图所示。

主机 范围 子网 地址组

地址范围属性

名称

起始地址

终止地址

排除地址

<-

×

确定

取消

参数说明如下表所示。

参数	说明
名称	指资源的名称。为必填项。
起始地址	输入地址范围的起始 IP 地址。为必填项。
终止地址	输入地址范围的终止 IP 地址。为必填项。
排除地址	指的是该资源不包括的某些 IP 地址，当需要多个 IP 地址时中间用空格分开。

点击“确定”完成范围资源的设定。

3) 修改资源属性

点击地资源对应的“修改”图标可以修改其属性。

4) 删除资源

如果资源对应的“删除”一列为图标，则表明该资源未被引用，点击“删除”图标可以删除该资源。如果资源对应的“删除”一列为图标，则表明该资源被引用，无法删除。

点击“清空”可以清除所有**未被引用**的地址范围资源。

7.1.3 设置子网资源

1) 选择**资源管理 > 地址**，选择“子网”页签，在右侧页面内显示已有的子网地址资源，如下图所示。

主机

范围

子网

地址组

+

添加

🗑️

清空

总计: 3

名称	IP地址	掩码地址	除去地址	操作
rd_group	10.10.11.0	255.255.255.0	10.10.11.2 10.10.11.3	 
子网100.X	192.168.100.0	255.255.255.0		 
10.10.10.0	10.10.10.0	255.255.255.0		 

上图中，“删除”一列为表示该资源对象被规则引用，无法删除。

2) 添加资源

点击“添加”，系统出现子网属性的页面，如下图所示。

子网属性

名称 *

网络地址 *

子网掩码 *

排除地址 < X

确定 取消

参数说明如下表所示。

参数	说明
名称	指资源的名称。为必填项。
网络地址	输入子网 IP 地址。为必填项。
子网掩码	输入子网掩码地址。为必填项。
排除地址	指的是该子网资源不包括的某些 IP 地址，当需要多个 IP 地址时中间用空格分开。

点击“确定”完成子网资源的设定。

3) 修改资源属性

点击对应的“修改”图标可以修改已设定的子网资源。

4) 删除资源

如果资源对应的“删除”一列为图标“”，则表明该资源未被引用，点击“删除”图标可以删除该资源。如果资源对应的“删除”一列为图标“—”，则表明该资源被引用，无法删除。点击“清空”可以清除所有**未被引用**的子网资源。

7.1.4 设置地址组

不同的地址资源可以组合为一个地址组，用作定义策略的目的或源。地址组的支持增强了资源管理的层次性，使管理更加灵活。

设置地址组的步骤如下：

1) 选择 **资源管理 > 地址**，并在右侧页面内选择“地址组”页签，将会显示已有的地址组资源，如下图所示。

主机 范围 子网 地址组		
+ 添加 清空		总计: 1
名称	地址组成员	操作
地址组1	doc host1	 

上图中，如果“删除”一列为“—”表示该资源对象被规则引用，无法删除。

2) 点击“添加”，系统出现如下图所示的页面。

主机 范围 子网 地址组

地址组属性

名称

选择地址:

webservers [主机]

202.99.1.3 [主机]

202.98.1.3 [主机]

172.16.98.222 [主机]

DHCP Server [主机]

192.168.83.225 [主机]

192.168.83.220 [主机]

MAP_IP [主机]

->

x

成员:

确定

取消

参数说明如下表所示。

参数	说明
名称	指资源的名称。为必填项。
成员列表	选择该地址组包含的地址资源。 说明： “选择成员”右侧的排序按钮用于按照 ASCII 码的正序排列和倒序排列下面列表框中的对象。点击动态筛选按钮“”，左侧弹出文本框，管理员可以输入查询条件，则含有该字符的对象名称将被选中，可以方便用户按序查找资源。

点击“确定”完成地址组的设定，点击“取消”放弃添加。

3) 修改资源属性

点击“修改”图标可以修改已设定的地址组。

4) 删除资源

如果资源对应的“删除”一列为图标“”，则表明该资源未被引用，点击“删除”图标可以删除该资源。如果资源对应的“删除”一列为图标“—”，则表明该资源被引用，无法删除。点击“清空”可以清除所有未被引用的地址组。

7.2 设置区域资源

系统支持区域的概念，用户可以根据实际情况，将网络划分为不同的安全域，并根据其不同的安全需求，定义相应的规则进行区域边界防护。如果不存在可匹配的访问控制规则，网络卫士安全网关将根据目的接口所在区域的权限处理该报文。访问控制规则设置请参见[9.2访问控制规则](#)。

设置区域资源的具体操作如下：

1) 选择 **资源管理 > 区域**，显示已有的区域资源。安全网关出厂配置中缺省区域资源为area_eth0，并已和缺省属性资源eth0 绑定，而属性资源eth0 已和接口eth0 绑定，因此出厂配置中安全网关的物理接口eth0 已属于区域area_eth0。

区域					
 添加		 清空		总计: 4	
名称	绑定属性	权限	注释	操作	
area_eth0	eth0	禁止			
area_eth1	eth1	允许			
area_eth2	eth2	允许			
area_eth3	eth3	允许			

上图中，“删除”一列为“—”表示该资源对象被规则引用，无法删除。

2) 点击“添加”，增加一个区域资源，如下图所示。

区域

名称

*

访问权限

允许

注释

可用属性:

eth0

eth1

eth2

eth3

adsl

->

x

成员:

确定

取消

参数说明如下表所示。

参数	说明
名称	指资源的名称。为必填项。
访问权限	设定该区域的缺省访问权限（允许访问或禁止访问）。
注释	输入必要的说明信息。为可选项。
选择属性	选择与该区域绑定的属性。可以同时选择一个或多个属性。

设置完成后，点击“确定”按钮，完成区域资源的设置。点击“取消”则放弃添加，返回上一界面。

3) 修改资源属性

若要修改区域资源的设置，点击该区域资源所在行的“修改”图标，可以修改其属性。

4) 删除资源

如果资源对应的“删除”一列为图标“”，则表明该资源未被引用，点击删除图标可以删除该资源。如果资源对应的“删除”一列为图标“—”，则表明该资源被引用，无法删除。也可以点击“清空”一次删除所有**未被引用**的区域资源。

7.3 设置时间资源

用户可以设置时间资源，以便在访问控制规则中引用，从而实现更细粒度的控制。比如，用户希望针对工作时间和非工作时间设置不同的访问控制规则，引入时间资源的概念很容易解决此类问题。

时间资源根据使用的次数分为多次时间资源和单次时间资源，多次时间是指循环的时间对象，如每周的某一天、每日的某一时段，单次时间是指某一特定时段。

7.3.1 设置多次时间对象

1) 选择 **资源管理 > 时间**，选择“时间多次”页签，系统出现如下页面。

时间多次 时间单次					
 添加		 清空		总计: 1	
名称	星期	每日开始	每日结束	操作	
work_time	12345	09:00	17:30	 	

上图中，“删除”一列为“—”表示该资源对象被规则引用，无法删除。

2) 添加资源

点击“添加”，如下图。

时间属性

名称 *

每周时段

星期一 ☐
 星期二 ☐
 星期三 ☐
 星期四 ☐
 星期五 ☐
 星期六 ☐
 星期日 ☐

每日时段

开始时间 时 分 *
 结束时间 时 分 *

确定
取消

参数说明如下表所示。

参数	说明
名称	指资源的名称。为必填项。
每周时段	选择每周的哪天。
每日时段	设置每天的起始时间和结束时间。 说明： 开始时间和结束时间使用的是 24 小时格式输入，如晚上 10 点，需要输入 22 时 00 分。

点击“确定”，完成设置。新添加的资源将显示在时间资源列表中。

3) 修改资源属性

对已经添加的时间资源，可以点击“修改”图标修改其属性。

4) 删除资源

如果资源对应的“删除”一列为图标，则表明该资源未被引用，点击“删除”图标可以删除该资源。如果资源对应的“删除”一列为图标，则表明该资源被引用，无法删除。管理员也可以点击“清空”一次性删除所有未被引用的资源。

7.3.2 设置单次时间对象

1) 选择 资源管理 > 时间，选择“时间单次”页签，系统出现如下页面。

时间多次		时间单次	
+ 添加		🗑️ 清空	
总计: 0			
名称	开始时间	结束时间	操作

上图中，“删除”一列为“—”表示该资源对象被规则引用，无法删除。

2) 点击“添加”，设置单次时间资源，如下图。

时间单次

时间属性

名称

开始时间

年 2009 月 01 日 01

时 00 分 00 秒 00

结束时间

年 2009 月 01 日 01

时 00 分 00 秒 00

确定

取消

参数说明如下表所示。

参数	说明
名称	指资源的名称。为必填项。
开始时间	设置从具体哪天的哪个时刻开始算起。 说明： 使用 24 小时格式输入，如晚上 10 点，需要输入 22 时。
结束时间	设置到具体哪天的哪个时刻为止。 说明： 使用 24 小时格式输入，如晚上 10 点，需要输入 22 时。

最后点击“确定”，完成资源设置。新添加的资源将显示在时间资源列表中。

3) 修改资源属性

对已经添加的时间资源，可以点击“修改”图标修改其属性。

4) 删除资源

如果资源对应的“删除”一列为图标“🗑️”，则表明该资源未被引用，点击“删除”图标可以删除该资源。如果资源对应的“删除”一列为图标“—”，则表明该资源被引用，无法删除。管理员也可以点击“清空”一次性删除列表中所有未被引用的资源。

7.4 设置服务资源

服务资源的设置便于用户根据不同的服务定义访问控制规则，服务资源分为三种：

- 系统定义服务：系统预定义的一些常用服务；
- 自定义服务：根据自身业务的需要自定义的服务和端口号；
- 服务组：将各种服务组合定义成服务组。

7.4.1 预定义服务

系统已预先定义了一些常见服务供用户在设置访问控制规则时使用。对于这些预定义的服务，用户不可以进行修改和删除，只能通过选择 **资源管理 > 服务**，选择“预定义”页签来进行查看，如下图所示。

预定义 自定义 服务组	
预定义服务	
总计: 194	
名称	详细
IP	ETH/0x0800
ARP	ETH/0x0806
LOOP	ETH/0x0060
XEROX_PUP	ETH/0x0200
PUPAT	ETH/0x0201
X25	ETH/0x0805

7.4.2 自定义服务

用户可以根据需要自行定义服务，操作方法如下：

- 1) 选择 **资源管理 > 服务**，选择“自定义”页签，右侧显示管理员添加的自定义服务，如下图所示。

预定义 自定义 服务组		
+ 添加 清空		
总计: 1		
名称	详细	操作
webport	TCP/8080	 

上图中，“删除”一列为“—”表示该资源对象被规则引用，无法删除。

- 2) 添加服务资源

点击“添加”，系统出现如下页面。



The image shows a dialog box titled "服务属性" (Service Properties). It contains three input fields: "名称" (Name) with a text box, "类型" (Type) with a dropdown menu showing "TCP", and "端口" (Port) with two text boxes separated by a hyphen. There are red asterisks next to the "名称" and "端口" fields. Below the fields is a note in brackets: "[单个端口或范围, 单个端口只填起始. ICMP是类型值0-18及特征码]". At the bottom are two buttons: "确定" (OK) and "取消" (Cancel).

参数说明如下表所示：

参数	意义
名称	输入自定义服务对象名。
类型	选择自定义服务使用的协议类型。可选值为：TCP、UDP、ICMP、以太网协议、其他 IP 协议。
端口	当“类型”选择 TCP、UDP、ICMP 时显示该选项。用于输入自定义服务占用的单个端口或端口范围，前后两个文本框分别表示起始和终止端口号。如果是单个端口则只填起始端口。 当协议类型为 TCP 或 UDP 时，可输入的数值范围为 0-65535。当协议类型选择 ICMP 时，可输入数值范围为 0-18；
类型值	当协议类型为“以太网协议”或“其他 IP 协议”时，界面显示该项。对于“以太网协议”，可输入的数值范围为 256-65535；对于“其他 IP 协议”，可输入的数值范围为 1-255。

点击“确定”，完成设置。点击“取消”放弃添加。

3) 修改资源属性

对已经添加的服务资源，可以点击“修改”图标修改其属性。

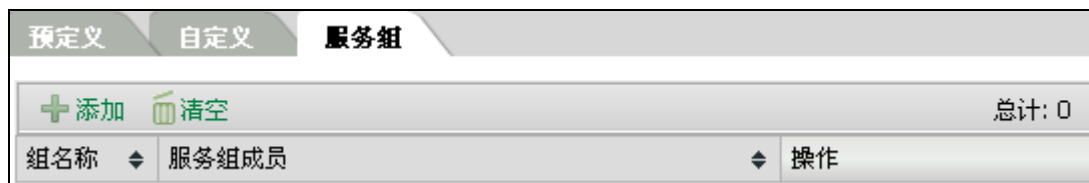
4) 删除资源

如果资源对应的“删除”一列为图标“”，则表明该资源未被引用，点击“删除”图标可以删除该资源。如果资源对应的“删除”一列为图标“—”，则表明该资源被引用，无法删除。管理员也可以点击“清空”一次性删除列表中所有的**未被引用**的资源。

7.4.3 设置服务组

用户可以灵活地将几个服务组合在一个服务组中，在设置访问控制时可以引用该服务组对象。

1) 选择 **资源管理 > 服务**，并激活“服务组”页签，如下图所示。



上图中，“删除”一列如果显示为“—”表示该资源对象被规则引用，无法删除。

2) 点击“添加”，系统出现设置服务组的页面，如下图所示。



参数说明如下表所示：

参数	意义
名称	输入服务组对象名。
服务成员列表	选择组成员，服务组中可以同时包括系统定义服务和用户自定义服务。

点击“确定”，即可生成新的服务组。

3) 修改资源属性

对已经添加的服务组资源，可以点击“修改”图标修改其属性。

4) 删除资源

如果资源对应的“删除”一列为图标，则表明该资源未被引用，点击“删除”图标可以删除该资源。如果资源对应的“删除”一列为图标“—”，则表明该资源被引用，无法删除。管理员也可以点击“清空”一次性删除列表中所有的未被引用的服务组资源。

7.5 设置域名对象

域名对象定义网络域名（DNS）关键字对象。通过定义域名对象并在访问控制规则中引用域名对象，可以实现基于域名的访问控制。域名过滤的工作原理是：

当客户端通过安全网关向指定域名发出连接请求时，IE 自动调用域名查询，向 DNS 服务器发送域名请求报文，当 DNS 服务器的回应报文通过安全网关时，如果定义了域名对象，则安全网关将在域名对象中记录域名对应的所有 IP 地址。如果管理员在访问控制策略中引用域名对象，则只要目的 IP 属于该 DNS 对象的 IP 地址池，报文就匹配 ACL 规则，安全网关将按照规则的权限对报文进行处理，从而实现基于域名的访问控制。

说明

- ◇ DNS过滤需要在ACL规则中调用DPI的DNS解析功能。而DNS解析功能，只有在绑定了端口后，才知道哪个端口上的流量是DNS的，因此，必须要绑定DNS服务端口，DPI DNS才能正常工作，DNS过滤也才能工作。服务端口绑定请参见 [10.4应用端口绑定](#)。

设置域名对象的步骤如下：

- 1) 选择 **资源管理 > 域名对象**，如下图所示。

名称	关键字	描述信息	操作
dns1	www.sina.com		

- 2) 点击“添加”，系统出现设置域名对象的页面，如下图所示。

参数说明如下表所示：

参数	意义
名称	输入域名对象名称。
描述	可选项，输入对该对象必要的描述信息。

参数	意义
关键字	输入域名格式的字符串。 说明： 关键字要符合域名的规范，简单的说只能包含数字、字母、下划线(_)、横杠(-)、点(.),总长度不能超过 256。

点击“确定”，即可生成新的域名对象。

3) 修改资源属性

对已经添加的域名对象资源，可以点击“修改”图标修改其属性。

说明

✧ 域名的属性中“名称”属性不能修改。

4) 删除资源

点击对应的“删除”图标可以删除该资源（已被引用的资源无法删除）；点击“清空”可以删除列表中所有**未被引用**的域名资源。

8 用户认证

TOS 系统可以实现有效、快速、全面的对远程接入的用户进行认证，支持本地证书认证、本地密码认证、外部服务器认证、第三方 CA 证书认证等认证方式，进而基于角色向用户授权可以访问的内网资源。对于 SSLVPN 用户和 VRC 用户，还可以基于用户进行资源授权。安全网关还可以对接入的认证客户端进行端点安全检测，如果客户端的某些安全因素不满足设定的规则，则不允许远程接入。

本章介绍远程接入的用户相关的所有信息配置，包括如下内容：

- 用户管理：介绍管理员如何对本地密码认证的远程用户进行添加、编辑、删除、启用、禁用等操作。
- 用户角色设置：介绍管理员如何对用户角色（即用户组）进行添加、编辑、删除等操作。
- 外部认证设置：介绍如何设置外部认证服务器的相关参数。
- 认证设置：介绍如何将外部认证服务器和证书服务器上用户映射为本地角色，则外部用户具有本地角色的相应权限。
- 可信接入：介绍如何设置接入端点安全的审查规则，并为角色或用户添加安全规则。

说明

- ✧ 认证成功还需要在安全网关的相关接口开放相关的认证服务，具体请参见[4.2.2.2开放服务](#)。
- ✧ 对于 CGI 认证用户，当对其配置了可信接入的安全规则组时，登录设备需要安装 ActiveX 控件。因此使用 IE 以外的其余浏览器登录设备时，请确认您的浏览器可以正确下载 ActiveX 控件，并正确安装控件，然后重新登录。否则系统将自动注销用户。
- ✧ SSL VPN 用户不支持使用 IE 以外的其余浏览器登录设备。
- ✧ 网络卫士安全网关对通过设备的用户采用集中认证、分布授权的方法，对于使用 Topsec 认证客户端登录安全网关的远程用户，或者 PPTP、L2TP 远程用户，选择菜单 **防火墙 > 访问控制**，使用访问控制规则基于用户角色进行权限控制；对于 SSL VPN 远程接入用户，则选择菜单 **SSL VPN > ACL 控制策略**，分别基于用户和角色进行授权；对于 IPSecVPN 用户，则选择菜单 **虚拟专网 > VRC 管理**，可以通过设置权限对象，并分别基于用户和角色进行授权。如果在“VRC 基本管理”中开启了“防火墙联动”功能，则还可以对 VRC 用户基于访问控制规则进行权限控制。

8.1 用户管理

网络卫士安全网关可以作为认证服务器，实现对远程用户的用户名密码认证。管理员需要首先在本地数据库中配置用户信息，进而设置该用户所属的角色，基于角色设置访问控制规则，实现对用户的资源授权。

用户身份认证的方式可以分为用户名密码认证和证书认证两种，用户的认证方式不同，资源授权的方式也有所不同。

➤ 用户名密码认证

当采用用户名密码认证方式时，根据认证服务器是否为安全网关设备，分为本地密码认证和外部密码认证（Radius、TACACS、SecurID、LDAP 和 TP）。

a) 对于本地密码认证的远程用户，都可以基于所属的角色进行访问权限控制。对于 SSL VPN 和 IPSecVPN 用户，可以同时基于用户和角色进行访问权限控制。当一个用户属于若干个角色时，按照角色的先后顺序进行访问控制规则匹配。一旦发现匹配的 ACL 规则，设备将停止匹配检查，并根据最先匹配的那一条规则对用户进行访问控制。

b) 对于采用外部服务器认证的远程用户，需要先将外部认证服务器上的用户按照管理员设定的属性映射到本地认证数据库的角色上，然后基于角色进行访问权限控制。用户属性映射请参见[8.4 认证设置](#)。

➤ 证书认证

当采用证书认证方式时，根据签发证书的 CA 是否是设备本身，分为本地证书认证、第三方 CA 离线认证、第三方 CA 在线认证三种。

当远程用户采用证书认证方式时，需要管理员将用户按照证书中的某个属性映射到本地数据库中的角色上，然后基于角色进行访问权限控制。证书属性映射请参见[8.4 认证设置](#)。

本节主要介绍本地数据库中用户信息的配置，包括用户信息的查询、添加、编辑、删除、清空，用户所属角色的设置等操作。

说明

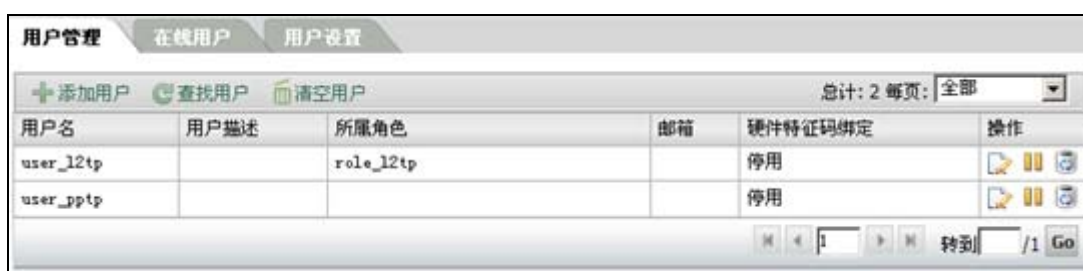
- ✧ 网络卫士安全网关对外部服务器认证的所有用户，根据映射策略设置其对应的本地角色，所有用户具有和角色一致的权限。如果对外部服务器认证的某个用户进行特殊的访问权限控制，需要在本地数据库中添加同名的“外部口令认证”用户，并设置其所属的用户角色，基于角色对外部认证的用户进行单独的访问控制。

- ✧ 当用户使用本公司的 TOPSEC 认证客户端软件登录安全网关时，只有导入 DER 格式的证书才能认证成功，导入 PEM、PKCS12 格式的证书不能认证成功。

8.1.1.1 配置用户

具体操作如下：

- 1) 选择 **用户认证 > 用户管理**，选择“用户管理”页签，界面显示已有的用户列表，如下图所示。



- 2) 点击“查找用户”按钮，管理员可以分类查找用户信息，界面如下图所示。



管理员可以按照用户的名称、电话号码、邮箱地址、状态是否禁止、描述信息、是否允许多点登录这六个方面来查找用户的信息，管理员只需选择相应页签，在下面的文本框中输入或在列表框中选择查找信息，点击“查找”按钮，则相应的用户信息将显示在 WEBUI 主界面中。

- 3) 添加新用户。

- a) 点击页面右上方的“添加用户”，进入添加新用户界面，如下图所示。



The dialog box is titled "用户属性" (User Properties). It contains the following fields and controls:

- 用户名** (Username): A text input field with a red asterisk indicating it is required.
- 用户描述** (User Description): A text input field.
- 认证方式** (Authentication Method): A dropdown menu currently showing "本地口令认证" (Local Password Authentication).
- 口令** (Password): A text input field with a red asterisk and the requirement "[6-31个字符]" (6-31 characters).
- 确认口令** (Confirm Password): A text input field with a red asterisk.
- 可用角色** (Available Roles): A list box on the left.
- 所属角色** (Assigned Roles): A list box on the right.
- Between the role list boxes are two buttons: "->" (Add) and "X" (Remove).
- 高级** (Advanced): A checkbox that is currently unchecked.
- At the bottom are two buttons: "确定" (OK) and "取消" (Cancel).

用户属性的参数说明如下表所示。

参数	说明
用户名	指认证用户的名称。为必填项，否则系统会弹出提示界面，且无法添加成功。 说明： 可以是中文字符、英文字母，下划线、横杠、数字的随意组合。最长 31 个字符。如果使用了“证书认证”、“本地口令+证书认证”或“外地口令+证书认证”的认证方式，则需要添加一个与证书 SUBJECT 域名称相同的用户。
用户描述	指认证用户的描述信息。为可选项。
认证方式	选择新添加用户的认证方式，可选项为： (1) 本地口令认证：表示在安全网关上进行认证，认证方式为用户名加密码认证方式； (2) 外部口令认证：表示在外部服务器上进行认证，认证方式为用户名加密码认证方式。只有需要对外部认证的用户进行单独授权时需要在本地数据库中添加外部口令认证的用户。此时还需要设置外部服务器信息，并将外部用户映射为本地角色。 (3) 证书认证：表示对用户采用证书进行身份认证。 (4) 本地口令+证书认证：表示在安全网关上进行认证，认证方式为用户名密码+证书认证方式。 (5) 外地口令+证书认证：表示在外部服务器上进行认证，认证方式为用户名密码+证书认证方式。只有需要对外部认证的用户进行单

参数	说明
	独授权时需要在本地数据库中添加外部口令认证的用户。
口令	指认证用户的认证密码。为必填项。最少 6 个字符，最长 31 个字符。只有“本地口令认证”和“本地口令认证+证书认证”这两种认证方式时才可添加。
确认口令	指再次输入认证用户的认证密码。为必填项。
可用角色	设置该用户所属的角色，则用户具有该角色的访问控制权限。当一个用户属于若干个角色时，“所属角色”中角色的前后排列顺序决定授予用户权限的顺序。一旦发现匹配用户的角色，设备将停止匹配检查，并根据最先匹配的那一个角色对用户进行授权。 说明： （1）“所属角色”中显示所有角色信息，管理员可以在“所属角色”中选择一个或多个角色，点击按钮“->”添加到“已经选择”中。根据添加顺序来决定“已经选择”中角色的排列顺序。也可以在“已经选择”中选择一个或多个用户组，点击按钮“×”从“已经选择”中删除。 （2）每个用户最多可以属于 16 个用户角色。

b) 选择“高级配置”，可以设置用户的高级属性，界面如下图所示。

高级	☒
用户邮箱	
用户手机号码	
登录地址范围	[IP地址]
	[掩码地址]
用户有效期	[起始时间]
	[结束时间]
	[格式:YYYY-MM-DD HH:MM:SS]
指定VIP地址	
用户状态	启用
是否允许用户修改密码	允许
硬件特征码绑定	停用
IPsecVPN认证配置	
客户端版本控制	默认
SSLVPN认证配置	
是否允许多点登录	允许
确定 取消	

用户高级属性的参数说明如下表所示。

参数	说明
用户邮箱	指认证用户的电子邮件地址信息，为可选项。
用户手机号码	指认证用户的手机号码。为可选项。
登录地址范围	指限制用户登录设备的 IP 地址及其掩码。IP 地址可以限定具体 IP 地址或输入子网地址。
用户有效期	设置该用户信息有效的时间范围，此处设定的时间范围之外该用户信息无效。
指定 VIP 地址	为用户接入指定虚拟网卡的地址。不能设定为本地球网已有的子网地址。
用户状态	设置该用户帐号是否允许使用，可选项为“启用”、“停止”。只有当选择“启用”时才可能允许该用户登录设备进行认证。
是否允许用户修改密码	设置是否允许用户修改自己的密码信息。 可选值：允许、不允许。
硬件特征码绑定	是否使用硬件特征码绑定功能，特征码是按照特定计算机硬件计算出来的特征值，不同计算机特征码不同。启用该功能后，将用户名和特定机器绑定在一起，减少内网资源被非授权访问的风险。
硬件特征码	输入硬件特征码，32 位 16 进制数。只有启用“硬件特征码绑定控制”时才可添加。该选项可以为空。 说明： 1. 当此处设置为非空的 32 位 16 进制数时，客户端的特征码必须与此处设定的一致，否则无法认证成功。 2. 此处设置为空时，安全网关根据客户端首次登录设备时使用的硬件特征码与该用户绑定，此后该用户只能通过初次登录主机登录安全网关设备。 3. 对于 VRC 用户，管理员可以在 VRC 客户端通过点击 帮助> 关于 菜单获取客户端的硬件特征码。
客户端版本控制	设置是否对 VRC 客户端采用的版本类型进行控制。可选项为默认、控制、不控制。 说明： 1. 设置为“默认”时，表示对该 VRC 客户端是否使用版本控制、使用哪个版本的设置，应当与 VRC 管理模块的基本设置模块关于 VRC 客户端版本控制的设置相一致，具体请参考《TopGate 管理手册——IPSec VPN 配置》手册。 a) 首先查看用户角色的设置，当角色设置为“控制”时，将要求客户端的版本号与用户角色处关于版本的设定一致；当角色设置为“不控制”时，对该 VRC 客户端不使用版本控制。 b) 当用户不属于任何角色时，要求客户端的版本号与 VRC 管理的“基本设置”中的设定一致。 2. 设置为“控制”时，表示 VRC 客户端使用的版本应当与此处设定的版本相一致，才可以登录认证成功。 此时需要选择“客户端版本”。目前支持的客户端版本类型有：标准版、标准版+“需要 UKEY”、标准版+“连上 VPN，禁止上网”、

参数	说明
	限制版、限制版+“需要 UKEY”。 3. 设置为“不控制”时，表示对该 VRC 客户端不使用版本控制。
客户端版本	选择 VRC 客户端使用的版本号，只有在客户端版本控制处选择“自定义”时才需要设置该项，此处应当与自身选购的 VRC 版本相一致。目前支持的客户端版本类型有：标准版、安全版、限制版、UKEY、安全版+UKEY、限制版+UKEY。
是否允许多点登录	对于 SSL VPN 用户，设置是否允许多个人使用同一帐号在不同地点登录。默认为“允许”。 说明： 当设备不包含 SSL VPN 模块时，界面不会显示该选项。

c) 设置完成后，点击“确定”按钮，添加一个新用户。或点击“取消”，放弃设置。

4) 启用、禁用用户。对于处于“启用”状态的用户，点击“状态”一系列的“禁用”图标可以禁用该用户，禁用后该用户信息将无效，如果该用户当前在线，则禁用该用户后会强制其下线。对于被禁用的用户，管理员可以点击“启用”图标重新启用该用户。

5) 修改或删除用户信息。

如需修改或删除，点击相应图标即可。

6) 清空用户信息。

点击页面右上方的“清空用户”，可以一次清空设备中所有用户信息。

8.1.1.2 查看在线用户

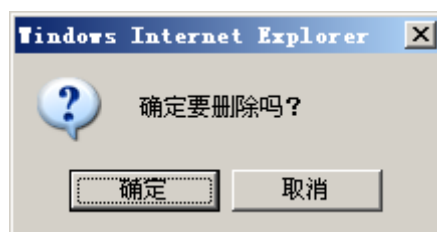
选择“在线用户”页签，显示当前登录安全网关的认证用户的信息，包括通过 TOPSEC 认证客户端登录的普通用户、OTP 用户及证书认证用户，PPTP 认证用户、L2TP 认证用户、VRC 用户以及通过 IE 浏览器登录设备的 CGI 认证用户等认证用户的信息，包括用户名、地址、服务器、登录时间。

说明

- ✧ 对于 VRC 用户，只有当开启“与防火墙联动”开关后才会显示在线的 VRC 用户信息，否则只在 VRC 模块的“在线用户”处显示，不在此处显示。

用户管理 在线用户 用户设置						
						总计: 1
用户名	地址	服务器	在线时间(HH:MM:SS)	类型	删除此地址	删除此用户
doc	192.168.83.224	localdb	0:0:7	cgi		

点击“删除此地址”对应图标，在如下图的对话框中点击“确定”可以强制从特定地址登录的该在线用户下线。



点击“删除此用户”对应图标，则会强制所有多点登录的同一用户下线。

8.1.1.3 用户设置

选择“用户设置”页签，用于管理员在设置用户口令时的安全机制，以及用户登录安全网关进行身份认证时的安全限制。管理员安全设置请参见 [4.4.2配置管理](#)。界面如下图。

用户管理 在线用户 用户设置	
认证参数	
同一用户最大登录地点	10 * [不大于2000个]
密码找回的通知方式	禁止 ▼
口令策略	
口令强度	弱 ▼ 口令无特殊要求
首次登陆修改密码	否 ▼
口令最小长度	6 * [受口令强度限制]
口令过期时间	0 * [30-90天, 默认永不过期]
应用	

参数说明如下表所示：

参数	说明

参数	说明
同一用户最大登录地点	设定允许同名认证用户从不同地点（IP）登录设备的最大值。
密码找回的通知方式	设定当本地认证的用户忘记密码时，在默认邮件和短信都是安全的前提下，是否允许进行用户密码找回工作，并设置找回密码方式。 拒绝执行密码找回操作。 2) 执行密码找回操作的客户端，必须通过右键菜单进行简单的验证码的输入操作，防止进行自动攻击的操作发生。 说明： 1. 用户最多可以有 10 次找回密码的机会，超过 10 次后系统将拒绝执行密码找回操作。 2. 执行密码找回操作的客户端，必须通过右键菜单进行简单的验证码的输入操作，防止进行自动攻击的操作发生。
口令强度	设置添加用户时口令强度的强弱程度。可选项为：弱、中、强。 说明： 设置为“弱”时，只有口令长度的限制，没有口令复杂度限制； 设置为“中”时，有口令长度限制，且口令复杂度为：至少包含一个数字和至少包含一个小写字母； 设置为“强”时，有口令长度限制，且口令复杂度为：至少包含一个数字，至少包含一个小写字母，至少包含一个大写字母，而且至少包含一个数字和字母外的其他符号，且口令中不能包含用户名。
首次登陆修改密码	设置管理员首次登陆系统后是否必须修改密码。默认选项为“关”。点击“开”后，管理员首次登陆系统后必须修改密码。
口令最小长度	设置口令最小必须包含的字符数。可选项为 6 到 31。
口令过期时间	设置口令的有效期限。默认为 0，输入范围为 30 到 90。0 表示永不过时。单位为天。

点击“应用”完成参数设置。

8.2 用户角色设置

网络卫士安全网关基于角色对所有用户进行访问权限控制。对证书认证用户和外部认证服务器的用户，需要按照设定的属性将用户映射到本地数据库中的用户角色，根据本地角色来进行授权。对于本地密码认证的用户，也基于其所属的角色来进行权限分配。当一个用户属于若干个用户角色时，按照用户角色的先后顺序进行访问控制规则匹配。

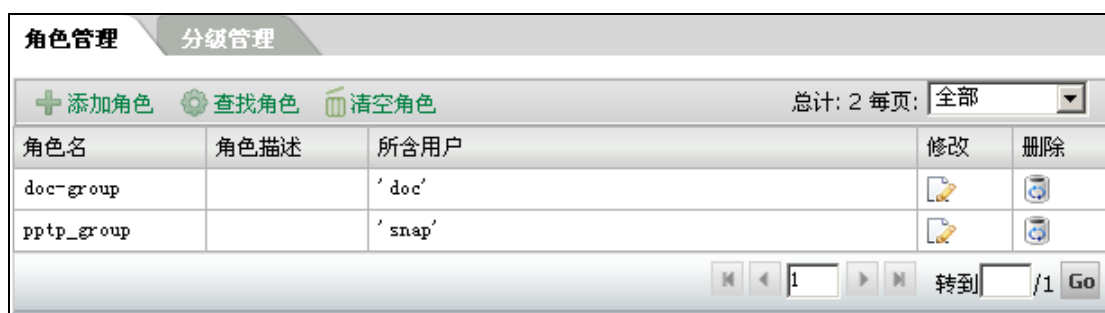
8.2.1 角色管理

管理员在此对用户角色信息进行管理和设置，包括新用户角色添加，已有的用户角色信息的编辑、删除、查找、清空等。还可以设置属于用户角色的用户信息。

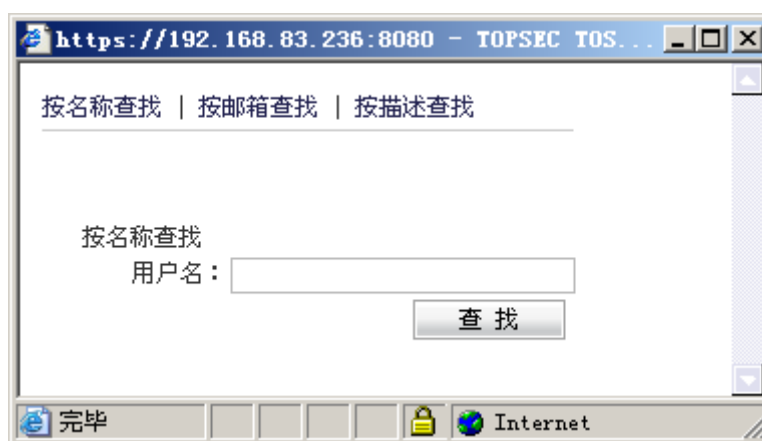
说明

- ✧ 设备最多支持 512 个用户角色，2048 个用户，所有用户角色中的用户总和不超过 2048 个。

1) 选择 **用户认证 > 用户角色**，并选择“角色管理”页签，界面显示已有的用户角色列表，如下图所示。



2) 点击“查找角色”按钮，管理员可以分类查找用户角色信息，界面如下图所示。



管理员可以按照用户的名称、邮箱地址、描述信息这三个方面来查找用户角色的信息，管理员只需选择相应页签，在下面的文本框中输入或在列表框中选择查找信息，点击“查找”按钮，则相应的用户信息将显示在 WEBUI 主界面中。

3) 添加用户角色信息。

点击页面右上方的“添加角色”，进入添加用户角色界面，如下图所示。

角色属性

角色名

*

角色描述

DHCP地址池

不添加

选择用户

test()

doc(111111)

已经选择

->

×

高级

☐

确定

取消

参数说明如下表所示。

参数	说明
角色名	指认证用户角色的名称。为必填项。
角色描述信息	指对该认证用户角色的描述信息。为可选项。
DHCP 地址池	为可选项。如果客户端登录安全网关后需要由安全网关为其分配 IP 地址，则需要安全网关上设置可分配的地址范围，即地址池。地址池可以在此处或 VRC 管理处设定，用户角色地址池设置优先于 VRC 管理处的设置。 说明： (1) 使用全网接入的用户角色必须配置该选项，否则该角色的用户无法获取 DHCP 地址池中的地址。 (2) 远程客户端进行全网接入时，从用户所属的角色中第一个设置地址池的用户角色为远程用户分配 IP 地址。该地址池必须是 DHCP 服务器上设定的地址池中的一个。
选择用户	设置属于该用户角色的用户信息。 “选择用户”中显示所有用户信息，管理员可以在左侧列表框中选择一个或多个用户，点击按钮“->”添加到右侧的“已经选择”列表中。也可以在右侧的“已经选择”列表中选择一个或多个用户，点击按钮“×”从本组用户中删除。

选择“高级配置”，可以设置用户的高级属性，界面如下图所示。

高级	☒
用户邮箱	
内部主DNS	
内部从DNS	
内部主WINS	
内部从WINS	
强制短信认证	否
IPsecVPN认证配置	
客户端版本控制	不控制

参数说明如下表所示。

参数	说明
用户邮箱	设置该角色的邮箱地址。可选项。
内部主/从 DNS	安全网关可以通过 DNS 服务器设置选项来设置客户端虚拟网卡的 DNS 地址。在“首选 DNS 服务器地址”，设置首选 DNS 服务器的 IP 地址。在“备选 DNS 服务器地址”，设置备选 DNS 服务器的 IP 地址。
内部主/从 WINS	安全网关可以通过 WINS 服务器设置选项设置客户端虚拟网卡的 WINS 地址。在“首选 WINS 服务器地址”，设置首选 WINS 服务器的 IP 地址。在“备选 WINS 服务器地址”，设置备选 WINS 服务器的 IP 地址。
强制短信认证	设置是否对属于该角色的用户使用短信认证方式。短信认证服务器设置请参见 4.2.6短信设置。 说明： - 手机短信认证是指安全网关在对用户身份进行确认过程中，用手机短信配合验证的一种认证方式。因此管理员必须在用户管理处设置“用户手机号码”，否则无法使用短信认证功能。 - 如果在 VRC 的“基本设置”处开启了“强制短信认证”，则表示所有的用户都必须进行短信认证，而不管角色里是否设置了短信认证。
客户端版本控制	设置是否对 VRC 客户端采用的版本类型进行控制，只有当用户配置的“客户端版本控制”选择“默认”时，VRC 的版本控制才会匹配本处的设置。可选项为控制、不控制。 说明： “控制”表示 VRC 客户端使用的版本应当与此处设定的版本相一致，才可以登录认证成功。此时需要选择“客户端版本”。目前支持的客户端版本类型有：标准版、标准版+“需要 UKEY”、标准版+“连上 VPN，禁止上网”、限制版、限制版+“需要 UKEY”。 “不控制”表示对该 VRC 客户端不使用版本控制。此时客户端

参数	说明
	的版本控制信息还要查看 VRC 管理处关于“客户端版本控制”的设置。
客户端版本	当“客户端版本控制”设置为“控制”时需要设置该项，用于限制 VRC 客户端使用的版本类型，只有符合规定版本的 VRC 用户才可以登录认证成功。 目前支持的客户端版本类型有：标准版、标准版+“需要 UKEY”、标准版+“连上 VPN，禁止上网”、限制版、限制版+“需要 UKEY”。

参数设置完成后，点击“确定”完成用户角色添加。

4) 修改用户角色信息。

点击待修改用户角色条目右侧的“修改”图标，可以修改该用户角色的基本信息。

5) 删除用户角色信息。

如果用户角色没有被引用，则点击待删除用户角色条目后的“删除”图标，可以删除该用户角色信息。

6) 清空用户角色信息。

点击页面右上方的“清空角色”，可以一次清空所有用户角色信息。

8.2.2 分级管理

分级管理员只具备查看和修改由他创建的用户权限，分级管理员配置请参见 [4.4.1配置管理员账号](#)。通过为分级管理员设置所属的角色，该管理员创建的用户均属于相应的角色。

为分级管理员设置角色的具体配置步骤为：

1) 选择 用户认证 > 用户角色，并选择“分级管理”页签，界面如下图所示。

角色管理 分级管理		
+ 添加		
分级管理员	角色	操作
gradeadmin	pptp_group	 

2) 为分级管理员设置角色

点击“添加”按钮，界面如下图所示。

选择分级管理员名称，并选择其所属的角色，点击“确定”按钮完成设置。

3) 点击“操作”一系列的“修改”图标可以修改分级管理员所属角色。

4) 点击“操作”一系列的“删除”图标可以删除分级管理员和角色之间的对应关系。

8.3 外部认证

网络卫士安全网关不仅能够作为认证服务器接受用户的认证请求，还可以转发用户向外部认证服务器提出的认证请求，此时需要在安全网关对外部认证服务器的连接信息（例如 IP 地址、端口号等）进行设置，并添加用户角色，将外部认证服务器上的用户映射为本地用户角色，然后基于角色对认证用户设置访问控制规则。网络卫士安全网关支持的外部认证协议包括 Radius、Tacacs、LDAP、SecuID、HTTP 协议，以及和 TP 服务器的联合认证。设置外部认证服务器的相关步骤介绍如下：

1) 在左侧导航菜单中选择 **用户认证 > 外部认证**，如下图所示。

外部认证				
+ 添加服务器		清空服务器		总计: 2
服务器名	测试	同步	修改	删除
radius_s1	-	-		
ldap				

如上图所示，只有 LDAP 服务器的“测试”和“同步”一列可以操作，点击“测试”图标可以测试安全网关与 LDAP 服务器是否连通；点击“同步”则可以根据设定的过滤条件，将 LDAP 服务器上的组和用户同步到安全网关的“用户角色”和“用户”列表中。

2) 添加外部服务器

a) 点击“添加服务器”，添加新的外部服务器信息，界面如下图所示。



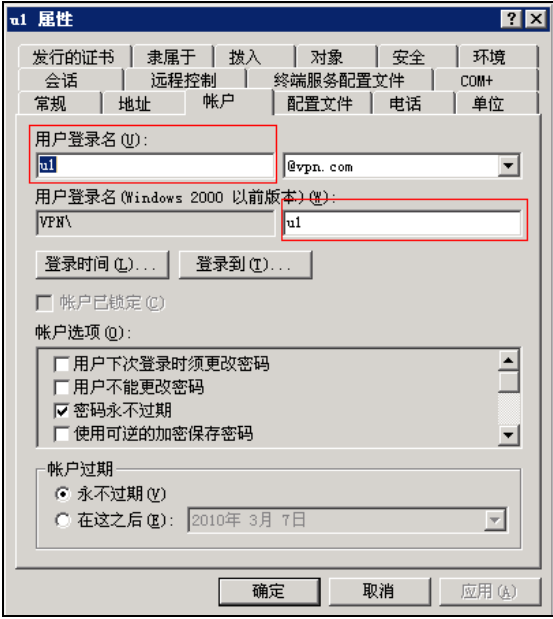
认证服务器属性配置界面，包含以下字段：

- 服务器名称：文本输入框，带红色星号 *
- 认证协议：下拉菜单，当前选择 RADIUS
- 服务器地址：文本输入框，带红色星号 *
- 服务器端口：文本输入框，当前值为 1812，带红色星号 *
- 超时时间：文本输入框，右侧提示 [1-180秒, 缺省为5秒]
- 预共享密钥：文本输入框，带红色星号 *
- 认证客户端地址：文本输入框
- 认证方法：下拉菜单，当前选择 PAP

底部有“确定”和“取消”按钮。

参数说明如下表所示。

参数	说明
服务器名称	输入外部认证服务器的名称。
认证协议	选择认证协议，可选值为 RADIUS、TACACS、LDAP、SECURID、TP 和 HTTP。 说明： TP 表示将 TP 服务器上的用户角色映射为 TOS 上的同名角色后，对角色进行访问控制；
服务器地址	指认证服务器的 IP 地址。
服务器端口	指认证服务器的监听认证请求的服务端口，不同协议的默认值不同。 如：Radius 协议默认为 1812。LDAP 协议默认为 389。
超时时间	为判断某个服务器是否失效，安全网关会向服务器周期性地发送请求报文，如果在规定的时间内未得到服务器发回的应答，需重传请求报文。范围为 5-180 秒，默认值为 5 秒。
预共享密钥	指认证服务器端的共享密钥。当认证协议选择 radius,tacacs 时必须设置该项。
认证客户端地址	仅当认证协议为 Radius 时需要设置该项，表示安全网关与 Radius 服务器连接的出接口的 IP 地址。
服务器 DN	指 LDAP 服务器的域名。需要输入域名分解格式，不同厂家的 LDAP

参数	说明
	服务器需要设置不同的关键字。例如：假设 AD 服务器域名为“sina.com”则此处应输入“dc=sina,dc=com”。 说明： 在LDAP服务器上可以通过“我的电脑”右键菜单的 属性 > 计算机名 来查看服务器所在的域。
认证方法	只有认证协议选择“Radius”时需要设置该项。指 Radius 认证协议的认证方法，可选值为 PAP、CHAP。
LDAP 查询用户	输入 LDAP 服务器上具有用户查询权限的用户 DN（一般为管理员 DN）。在配置管理员 DN 时，需要输入完全管理员的 DN，比如管理员是 Administrator，由于 Administrator 也属于 Users 用户组，则管理员 DN 为：cn=Administrator,cn=users,dc=cams,dc=com。 说明： 当进行 Windows 域认证（即 MS-AD 认证）时，请确保 Windows 域服务器中设置的用户的“用户登录名”和“用户登录名（windows 2000 以前版本）”具有相同的值，如下图。 对于两者不同的情况，请使用“登录名（windows2000 以前版本）”中所显示的用户名进行登陆。具体设置可咨询 Windows 域服务器的管理员。 
LDAP 查询口令	输入 LDAP 服务器上具有用户查询权限的管理员的密码。
服务器类型	LDAP 是一个开放的协议，不同的公司有不同的实现方法，因此需要选择 LDAP 服务器的类型，可选项为 MS-AD、sun、Novel 和 other。分别表示微软公司的 AD 服务器、sun 公司的 LDAP 服务器、Novel 公司的 LDAP 服务器和 s 其他公司的 LDAP 服务器。
LDAP 命名属性	输入 LDAP 服务器的用户名属性标识。只有当“服务器类型”选择“other”时需要管理员设置该参数。选择其它“服务器类型”时无需设置该参数，设置完成后点击“修改”图标可以查看到该参数已经设置好。

参数	说明
	说明： 在 Active Directory 中，用户名属性标识通常为：saMAccountName。
LDAP 查询范围	设置以服务器 DN 为起点，查询 LDAP 目录的范围。可选项为 subtree 和 onelevel。 说明： Subtree 表示对包含服务器 DN 的所有子节点都进行查询；onelevel 表示只对服务器 DN 的直接子节点进行查询。

b) 参数设置完成后，点击“确定”按钮，完成外部认证服务器的添加；点击“取消”按钮，取消此次添加操作。

c) 测试 LDAP 服务器配置是否成功



对于 LDAP 服务器，点击“测试”图标，可以测试 LDAP 服务器配置是否成功。界面如下图所示。



参数说明如下表所示。

参数	说明
服务器名	选择 LDAP 认证服务器的名称。
用户名	可选项，输入 LDAP 服务器上的用户名。如果不输入，则只利用服务器设置的查询用户测试与服务器是否连通；如果输入该选项，则进一步利用查询用户查询该用户是否存在。
密码	可选项，输入 LDAP 服务器上用户的密码。如果不输入，则只利用

参数	说明
	服务器设置的查询用户测试与服务器是否连通；如果输入该选项，则进一步利用查询用户查询该用户密码是否正确。

点击“确定”按钮，如果连接不正确则返回提示的错误信息；如果正确则没有任何提示信息。

d) 同步 LDAP 服务器上的组和用户

对于 LDAP 服务器，设置完成后可以点击“同步”图标，将 LDAP 服务器上的组和用户同步到安全网关的“用户角色”和“用户”列表中。界面如下图所示。

同步用户和角色

服务器名称

同步方式 自动

同步时间间隔 [1-24小时, 缺省为24小时]*

生成用户 ☐

用户属性 外部口令认证

多点登陆 ☐

特征码绑定 ☐

用户过滤条件

生成角色 ☐

角色过滤条件

确定
取消

参数说明如下表所示。

参数	说明
服务器名称	显示 LDAP 认证服务器的名称。
同步方式	选择手动或自动同步，选择“自动”时，还需要设置“同步时间间隔”，安全网关将按照设定的时间间隔向 LDAP 服务器获取用户及组信息。
同步时间间隔	同步方式为“自动”时，还需要设置“同步时间间隔”，网络卫士安全网关将按照设定的时间间隔向 LDAP 服务器获取用户及组信息。
生成用户	设置是否将 LDAP 服务器的用户同步到安全网关上。勾选该选项后，点击“确定”按钮后，将按照“用户过滤条件”设定的条件过滤 LDAP 服务器上的用户，在“用户管理”页签可以查看到已经生成的 LDAP 用户。
用户属性	设置用户的认证方式，可选项为“外部口令认证”和“外部认证+证书认证”。
多点登陆	设置是否允许多个人使用同一帐号在不同地点登陆。该选项仅对于 SSL VPN

参数	说明
	用户有效。 说明： 当设备不包含 SSL VPN 模块时，界面不会显示该选项。
特征码绑定	设置是否使用硬件特征码绑定功能，特征码是按照特定计算机硬件计算出来的特征值，不同计算机特征码不同。启用该功能后，将用户名和特定机器绑定在一起，减少内网资源被非授权访问的风险。
用户过滤条件	设置从 LDAP 服务器上同步用户时的过滤条件。例如：输入“saMAccountName=u*”时，勾选“生成用户”时，将只导入 LDAP 服务器上用户名以 u 开头的用户。 说明： 当设置多个过滤条件时，设置“或”关系时的格式为：（ （...）（...））； 设置“与”关系时的格式为（&（...）（...））。内层括号内设置具体的过滤条件。
生成角色	设置是否将 LDAP 服务器的组同步为安全网关上的用户角色。勾选该选项后，点击“确定”按钮后，将按照“角色过滤条件”设定的条件过滤 LDAP 服务器上的组，在“角色管理”页签可以查看到已经生成的 LDAP 用户角色，所有角色名称的前缀均为“ldap_”。
角色过滤条件	设置从 LDAP 服务器上同步组时的过滤条件。 说明： 当设置多个过滤条件时，设置“或”关系时的格式为：（ （...）（...））； 设置“与”关系时的格式为（&（...）（...））。内层括号内设置具体的过滤条件。

3) 修改服务器参数

对于已经添加的外部认证服务器，管理员可以点击“修改”图标对其参数进行修改。

4) 删除服务器

点击“删除”图标，可以删除该认证服务器。点击“清空服务器”按钮，可以一次性删除所有的认证服务器。

8.4 认证设置

远程用户登录安全网关进行认证时，网络卫士安全网关将按照一定的顺序，检索本地数据库和外部认证服务器中是否有匹配的用户名，对于外部认证用户，系统将根据最先匹配的映射策略将用户映射到本地用户角色上，网络卫士安全网关将依据事先设定的 ACL 规则对用户的访问权限进行控制。

本节主要介绍如何设置证书认证和外部认证的映射策略，以及如何调整映射策略的排列顺序。

具体设置方法为：

1) 选择菜单 **用户认证 > 认证设置**，如下图所示。

认证设置					
+ 添加映射		清空映射		总计: 2	
服务器名	状态	修改	上移	下移	删除
cert	启用	 外部属性映射	-	-	-
localdb	启用	-	↑	↓	-

上图中，“cert”为证书认证映射策略，始终排列在第一位。“Localdb”为系统内置本地密码认证的映射策略，默认排列在第二位。管理员手动添加的映射策略默认根据添加顺序进行排列。“状态”一列显示该策略是否有效，策略被“禁用”后将不再发生作用。

2) 添加新的映射策略

点击“添加映射”，管理员可以添加新的映射策略，如下图所示。

认证设置	
映射策略	
认证服务器	radius_server
启用	是
授权类型	本地角色集合映射
可用本地角色	顺序匹配角色
doc_role	
-> ×	
确定 取消	

参数说明如下表所示。

参数	说明
认证服务器	选择已经添加的外部认证服务器的名称。
启用	设置是否启用该认证策略。

参数	说明
	可选项：是，否；默认值为“是”。 说明： 当选择“否”后该映射策略将不生效,用户无法使用该服务器进行认证。
授权类型	设置组映射类型。 可选项为：“本地角色集合映射”和“外部属性映射”。 说明： 1) “本地角色集合映射”表示将外部服务器上的所有用户映射到 LocalDB 中某个用户角色上。 2) “外部属性映射”表示将外部认证服务器上的用户根据映射属性值映射为同名的本地用户角色，该用户的权限和 LocalDB 上对应用户角色的权限一致。
可用本地角色	当“授权类型”选择“本地角色集合映射”时显示该选项，设置将外部服务器上的所有用户映射到 LocalDB 中某个选定的用户角色上。 说明： 1) 此处可以选择多个用户角色，最多不能超过 4 个。 2) 当一映射到多个角色时，角色的前后排列顺序决定访问控制规则匹配顺序。一旦发现匹配用户的 ACL 规则，设备将停止匹配检查，并根据最先匹配的那一条规则对外部认证用户进行授权。
属性名称	当“授权类型”选择“外部属性映射”时显示该选项，设置根据此处设定的属性将认证服务器的用户映射到 LocalDB 中的同名用户角色上。 说明： 在配置完外部属性映射后，一定要在用户角色中创建与相应属性值对应的同名角色。

参数设置完成后，点击“确定”按钮，完成映射策略的添加；点击“取消”按钮，取消此次添加操作。

3) 修改属性

对于已经添加的外部认证服务器，管理员可以点击“修改”图标对其参数进行修改。

4) 删除服务器

对于管理员手工添加的服务器映射策略，可以点击“删除”图标将其删除。

需要注意的是，系统内置的cert和localdb映射策略无法删除。

5) 移动策略位置

由于映射策略执行顺序匹配原则，即策略的顺序与策略的逻辑相关，用户应该根据网络实际情况及时调整策略的位置进而改变映射策略的执行顺序。

管理员可以通过点击“上移”或“下移”来改变除了 cert 以外的映射策略的默认排列顺序。

6) 设置证书认证用户的映射属性

对 cert 服务器，管理员可以点击“修改”一系列的修改图标，可以设置证书用户的默认映射策略，如下图所示。

The dialog box titled "映射策略" (Mapping Strategy) contains the following fields and controls:

- 认证服务器** (Authentication Server): A dropdown menu with "cert" selected.
- 启用** (Enable): A dropdown menu with "是" (Yes) selected.
- 授权类型** (Authorization Type): A dropdown menu with "本地角色集合映射" (Local Role Set Mapping) selected.
- 可用本地角色** (Available Local Roles): A list box containing "doc", "manager", and "configer".
- 顺序匹配角色** (Order Matching Roles): An empty list box.
- Between the two list boxes are two buttons: "->" and "X".
- At the bottom are two buttons: "确定" (OK) and "取消" (Cancel).

点击“修改”一系列的“外部属性映射”图标，可以进一步设置特殊的证书认证用户的映射策略。

认证设置						
证书属性						
添加 清空		总计: 2				
序号	规则条件	角色列表	上移	下移	修改	修改
1	unit==topsec	doc				
2	city==beijing&&email==pt_mgr@topsec.com.cn	manager				

所有映射规则默认按照添加顺序排列，所有证书认证的用户将顺序检查列表中是否有匹配的规则，如果有，则符合条件的证书用户将具有设定角色的权限；否则用户将不具有角色的权限，只拥有用户权限。

a) 添加映射策略

点击“添加”，设置界面如下图所示。

外部映射属性

名称

等于

国家

等于

省

等于

城市

等于

组织

等于

单位

等于

邮箱

等于

逻辑关系

无

本地角色集合

doc

已经选择

->

×

确定

取消

参数说明如下表所示：

参数	说明
选择条件	在“名称”、“国家”、“省”、“城市”、“组织”、“单位”和“邮箱”处设置检测证书哪些字段的属性。
逻辑关系	当选择两个以上条件时，必须在“逻辑关系”处设置各个条件之间是“与”还是“或”的关系。设置为“与”，表示必须同时满足多个条件；当设置为“或”时则表示满足其中的一个条件即可。
本地角色集合	选择一个或多个本地角色。满足条件的证书用户将具有设置的本地角色的权限。

- b) 点击“上移”或“下移”一列对应的图标可以改变策略的顺序。
- c) 点击“修改”图标可以修改策略属性。
- d) 点击“删除”图标可以删除策略。

8.5 可信接入

目前导致安全事件的主要原因是主机软、硬件结构存在设计漏洞并且对用户没有进行严格的认证和授权控制，传统安全防范的重点放在对服务器和网络的保护上，而忽略终端接入者本身的安全。但大多数的攻击事件都是由终端接入者本身不安全而引起发的，所以只有从终端接入的源头就建立起安全体系，内外共防来构造真正安全可信的网络环境。

网络卫士安全网关接收到认证客户端的认证请求时，首先对客户端的身份进行认证，身份认证成功时，安全网关将根据对用户及角色设定的安全规则组，对客户端主机上的系统补丁和操作系统等进行安全检测，只有满足安全规则组设定的检测条件时才允许认证客户端接入设备。

安全策略检测时，首先检测用户安全策略，如果不满足用户安全检测策略，则安全网关将不允许认证客户端接入；只有当用户的设置满足安全策略设定的条件时，才进一步检查其所属角色的安全策略。当用户的设置满足所属角色的安全策略时，用户将同时获得用户和角色的访问权限；否则其只有用户的访问权限而不具有角色的访问权限。

8.5.1 安全规则

安全规则用于设置对客户端主机进行安全检测的具体规则，包括检测项目及其匹配条件。安全网关可以检测的项目包括系统补丁和操作系统，匹配条件根据检测项目的不同会有不同的设置参数。

安全规则的具体设置方法为：

1) 选择菜单 **用户认证 > 可信接入**，并选择“安全规则”页签，界面显示已经设置的安全规则，如下图所示。

安全规则						
安全规则组		用户策略	角色策略	检查方式		
+ 添加规则 G 查找规则 🗑 清空规则						总计: 0
规则名	规则类型	操作码	检测项	检测值	修改	删除

2) 点击“查找规则”，可以根据管理员指定的特征快速定位规则，弹出的查询界面如下图所示。

在上图界面中设定要查询的规则的名称、规则描述信息、检测类型和检测操作系统中的一项或多项后，点击“查找”按钮，符合条件的结果将显示在主界面下方的安全规则列表中。

3) 点击“添加规则”可以添加新的检测规则，界面如下图所示。

参数说明如下表所示：

参数	说明
规则名称	输入新规则的名称。
检测类型	选择检测项目，可选项为：注册表项、文件状态、文件版本、进程、端口、服务、系统补丁、操作系统、设备、杀毒软件。 说明： 当选择不同的检测类型时，需要设置不同的检测项和检测值。
检测操作系统	当“检测类型”选择“注册表项”、“文件状态”、“文件版本”、

参数	说明
	“进程”、“端口”、“服务”、“系统补丁”、“设备”、“杀毒软件”时需要设置该项。用于选择操作系统的值，当被检测机使用的操作系统不是规则设定的操作系统时，如果检测机满足此规则所属策略中的其他规则，此规则被忽略。如果策略中仅有一条或多条这样的规则，规则不能通过检测。
操作码	检测类型选择“注册表项”、“文件版本”“系统补丁”时需要设置该项。 说明： 选项为“等于”或“包含”，检测客户端主机中的“检测项”处设定的文件版本号等于或包含设定的检测值。
检测项	设置对客户端主机的详细检查项目，最多输入 255 个字符。设置不同的“检测类型”时，可选项不同： 1) 当检测类型选择“注册表项”、“文件状态”、“文件版本”、“进程”、“服务”时，需手动输入检测项； 2) 当检测类型选择“端口”时，需选择端口类型（TCP 或 UDP），并设置端口号； 3) 当检测类型选择“系统补丁”时，需选择为“系统大补丁”或“系统小补丁”； 4) 当检测类型选择“操作系统”时，可选项为“WIN95”、“WIN98”、“WINNT”、“WIN2000”、“WINXP”、“WIN2003”、“VISTA”、“WIN2008”、“WIN7”。 5) 当检测类型选择“设备”时，可选项为“无线接入”、“多网卡”。
检测值	设置对客户端主机的详细检测值，最多输入 255 个字符。设置不同的“检测类型”时，有不同的设置项目： 1) 当检测类型选择“注册表项”、“文件版本”时，需用户根据需要自行设置检测值； 2) 当检测类型选择“文件状态”、“进程”时，可选项为“存在”、“不存在”； 3) 当检测类型选择“端口”时，可选项为“监听”、“不监听”； 4) 当检测类型选择“服务”时，可选项为“未安装”、“安装”、“运行”、“停止”； 5) 当检测类型选择“系统补丁”时，检测项为“系统大补丁”的可选项为“Service Pack 1”、“Service Pack 2”、“Service Pack 3”、“Service Pack 4”；检测项为“系统小补丁”时需手动录入； 6) 当检测类型选择“操作系统”时，可选项为“是”、“不是”； 7) 当检测类型选择“设备”时，检测项为“无线接入”的可选项为“不检查”、“禁止 AP 接入”；检测项为“多网卡”的可选项为“不检查”、“禁止多网卡接入”； 8) 当检测类型选择“杀毒软件”时，可选项为“不检测”、“安装杀毒软件”、“有杀毒软件”、“禁止病毒库过期接入”。
描述信息	输入对该规则必要的描述信息，为可选项。

参数设置完成后，点击“确定”按钮，完成安全规则的添加，界面如下图所示。点击“取消”按钮，取消此次添加操作。

安全规则

安全规则组

用户策略

角色策略

检查方式

+ 添加规则

🔍 查找规则

🗑️ 清空规则

总计: 1

规则名	规则类型	操作码	检测项	检测值	修改	删除
win_98	操作系统	-	win98	是		

4) 修改安全规则。

点击修改图标，即可修改相应规则的参数。

5) 删除安全规则。

点击删除图标，即可删除相应规则。

点击页面右上方的“清空规则”，可以一次清空设备中所有**未被引用**的安全规则。

8.5.2 安全规则组

设置了安全规则之后，管理员必须将多个安全规则进行逻辑组合，建立安全规则组，才能对用户和角色设置安全检测策略。安全规则组就是对登录客户端进行是否可信检测的安全策略，当管理员进一步设置用户及角色的安全规则组时，设备自动将策略的各个规则按照设定的逻辑整合后，对登录客户端进行安全检测。

安全规则组的具体设置方法为：

1) 选择菜单 **用户认证 > 可信接入**，并选择“安全规则组”页签，界面显示已经设置的安全规则组，如下图所示。

安全规则		安全规则组		用户策略		角色策略		检查方式			
+ 添加规则组		🗑️ 清空规则组						总计: 0			
规则组名		规则对象		影响范围		逻辑关系		修改		删除	

2) 点击“添加规则组”可以添加新的安全规则组，界面如下图所示。

安全规则组

规则组名称

*

影响范围

局部

逻辑关系

与

可用规则

win_98

sp_2

成员

->

×

确定

取消

参数说明如下表所示。

参数	说明
规则组名称	输入规则组的名称。
影响范围	安全规则组应用于“角色”时该选项才有意义，应用于“用户”时该选项设置没有意义。可选项为“全局”、“局部”。 说明： 1) 当规则组设置为“全局”时，如果“用户角色”设置了该安全规则组，则如果用户端不满足该处设定的条件时，不允许该角色的用户登录设备；当满足条件时，该用户是否能获得该角色的相应权限，则还取决于该角色的其他安全规则组，只有同时满足所有的策略时才能授予该角色的权限。 2) 设置为“局部”时，如果“用户角色”设置了该安全规则组，则即使用户端不满足设定的条件，也允许通过设备，但不能授予该角色的权限。
逻辑关系	设置该规则组中的安全规则之间的逻辑关系，可选项为“与”和“或”。 选择“与”时，客户端的检测项目必须同时满足所有安全规则设定的条件，才表示客户端安全条件满足此规则组。 选择“或”时，客户端的检测项目只要满足其中一项安全规则设定的条件，即表示客户端安全条件满足此规则组。
选择规则	选择该规则组中包含的安全规则。列表中显示已经设置的安全规则。

参数设置完成后，点击“确定”按钮，完成安全规则组的添加；点击“取消”按钮，取消此次添加操作。

3) 删除规则组

点击对应的“删除”图标，可以删除某安全规则组。

点击页面右上方的“清空规则组”，可以一次清空设备中所有**未被引用**的安全规则组。

8.5.3 用户策略

设置安全规则组后，管理员即可为用户设定安全检查规则，即登录客户端应当满足的安全策略。当用户在安全网关认证成功后，首先检查用户安全策略，只有当客户端的设置满足安全策略设定的条件时，才进一步检查其所属角色的安全策略。

用户安全策略的设置方法为：

1) 选择菜单 **用户认证 > 可信接入**，并选择“用户策略”页签，界面显示本地数据库中已经设置的用户，默认情况下没有设定任何安全策略，如下图所示。

安全规则			安全规则组	用户策略	角色策略	检查方式
清空规则组						总计: 2
用户名	规则组					修改
doc						
snap						

2) 设置用户的安全检测策略

点击“修改”图标可以设置用户的安全检测策略，界面如下图所示。

安全规则	安全规则组	用户策略	角色策略	检查方式
安全规则组： 已经选择： -> x 确定 取消				

选择规则组。当选择多个规则组时，不管该规则组为全局规则组或局部规则组，只有当用户的满足此处设定的所有安全规则时，才允许该用户通过安全网关设备，否则将拒绝用户通过。

选择完成后，点击“确定”按钮完成安全策略设置，点击“取消”放弃此次设置。

3) 点击“清空规则组”，则管理员可以一次性清除对所有用户设置的安全规则组。

8.5.4 角色策略

设置安全规则组后，管理员即可为用户角色设置安全检查规则，即用户角色应当满足的安全策略。当用户在安全网关认证成功后：

1) 首先检查用户安全策略，只有当用户的设置满足安全策略设定的条件时，才进一步检查其所属角色的安全策略。

2) 当用户的设置满足所属角色的全局及局部安全策略时，允许用户登录设备，用户将同时获得用户和角色的访问权限；否则如果只满足全局策略而不满足局部策略，则允许用户登录设备，但其只有用户的访问权限而不具有角色的访问权限；如果不满足全局策略，则不允许用户登录设备。

用户安全策略的设置方法为：

1) 选择菜单 **用户认证 > 可信接入**，并选择“角色策略”页签，界面显示本地数据库中已经设置的用户角色，默认情况下没有设定任何安全策略，如下图所示。

安全规则		安全规则组	用户策略	角色策略	检查方式
 清空规则组					总计: 2
角色名	规则组				修改
doc-group					
pptp-group					

2) 设置角色的安全检测策略

点击“修改”图标可以设置角色的安全检测策略，界面如下图所示。



选择规则组。当选择多个规则组时，当用户的设置满足所属角色的全局及局部安全策略时，允许用户登录设备，用户将同时获得用户和角色的访问权限；否则如果只满足全局策略而不满足局部策略，则允许用户登录设备，但其只有用户的访问权限而不具有角色的访问权限；如果不满足全局策略，则不允许用户登录设备。

选择完成后，点击“确定”按钮完成安全策略设置，点击“取消”放弃此次设置。

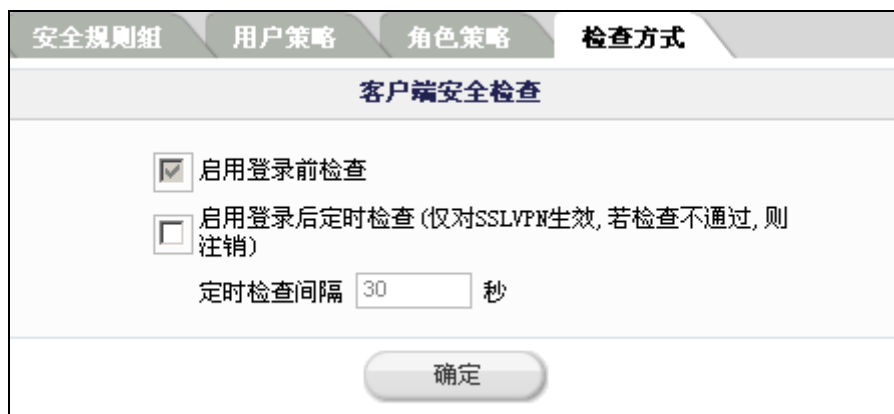
4) 点击“清空规则组”，则管理员可以一次性清除对所有角色设置的安全规则组。

8.5.5 检查方式

检查方式用于设置可信检查的策略，即设置在认证的时候就进行可信检查，还是在认证成功后定期进行可信检查。

具体设置方法为：

选择 **可信接入** > **检查方式**，界面如下图所示。



选择是否进行登录前检查，以及是否在登录后定时检查并设置定时检查的时间间隔。点击“确定”按钮完成设置。

9 防火墙

本章主要介绍如何实现数据报文的访问控制功能。用户可以通过地址转换策略控制内外网之间的访问，如限制外网用户对内网服务器的直接访问以及内网用户使用私有地址对外网的访问；通过报文阻断策略实现简单的二、三层访问控制；通过访问控制规则实现灵活、强大的三到七层的访问控制，用户还可以设置深度过滤策略针对应用层的内容进行更细颗粒度的访问控制。

通过阅读本章，用户可以了解如何通过设置地址转换策略、报文阻断策略以及访问控制规则进行数据流的控制。

本章内容主要包括：

- 报文阻断策略，介绍如何通过设置报文阻断策略，实现对二、三层的访问控制。
- 访问控制规则，介绍如何通过设置访问控制规则，实现对三到七层的访问控制。
- 访问记录，介绍如何查看访问权限类型为“收集”的访问控制规则相关的访问记录。
- 地址转换，介绍如何进行源、目的地址转换以及双向地址转换。
- IP/MAC 地址绑定，介绍如何将 IP 地址与 MAC 地址绑定从而防止非法用户冒充 IP 地址进行非法访问。
- 内容安全策略，主要介绍如何配置对各应用层协议的处理策略，如 HTTP 过滤策略、反垃圾邮件策略、应用程序识别策略等。

9.1 阻断策略

阻断策略实现对 IP 数据包的过滤，对 TopGate 需要转发的数据包，先获取数据包的包头信息，包括 IP 层所承载的上层协议的协议号、数据包的源地址、目的地址、源端口和目的端口等，以及数据包的二层协议类型、源和目的 MAC 地址信息，然后顺序和设定的阻断策略进行比较，根据比较的结果决定对数据包进行转发或者丢弃处理。如果没有匹配到任何策略，则会依据默认规则对该报文进行处理。在出厂配置中，默认阻断策略为允许所有的数据报文通过安全网关。

设置阻断策略的步骤如下：

1) 选择 **防火墙 > 阻断策略**，在右侧页面内显示已有的阻断策略和默认规则，如下图所示。

阻断策略											
+ 添加		清空		总计: 0							
ID	控制	二层协议	源MAC	目的MAC	三层协议	源IP	目的IP	源端口	目的端口	区域	日志
当前默认规则为: 允许通过不记录日志											

表中“ID”为每项策略的编号，在移动策略顺序时将会使用。“控制”中的图标绿色“√”和红色“×”，分别表示该项策略是允许还是禁止匹配条件的数据报文通过设备进行转发。点击“状态”栏的对应图标可以启用或禁用该规则。

点击“操作”一栏的对应图标可以修改规则属性、移动规则位置，或删除规则。

在出厂配置中，默认阻断策略为允许所有的数据报文通过安全网关，并且不记录日志信息。

2) 添加新的策略

a) 点击“添加”添加一条报文阻断策略，如下图所示。

阻断策略	
阻断策略属性	
访问权限	☒ 允许 ☐ 拒绝
日志记录	否
来源区域	---任意区域---
协议类型	IP
源MAC地址	[格式如 AA:BB:CC:DD:EE:FF]
目的MAC地址	[格式如 AA:BB:CC:DD:EE:FF]
IP协议类型	全部
源地址	--任意地址--
目的地址	--任意地址--
源端口	- [1-65535]
目的端口	- [1-65535]
确定 取消	

b) 设置基本参数，参数含义如下表所示。

参数	说明

参数	说明
访问权限	选择“允许”或“拒绝”符合该阻断策略的报文穿越安全网关。
日志记录	选择是否将阻断策略执行情况在日志中作记录。
来源区域	根据数据的源地址所属区域进行报文阻断。可以选择已经定义的区域对象或“任意区域”，“任意区域”表示不对报文所属的区域进行判定。
协议类型	根据协议类型进行报文阻断，包括 IP 协议、ARP 协议等。
源 MAC 地址	二层协议，源主机的 MAC 地址。MAC 地址中的字母十六进制数位应当大写。
目的 MAC 地址	二层协议，目的主机的 MAC 地址。在路由模式下，输入则只能为区域所属安全网关物理接口的 MAC 地址；在透明模式下，输入可以为目的主机的 MAC 地址。
IP 协议类型	三层协议，选择要过滤的协议类型，只有在“协议类型”处选择“IP”时，才需要设置该参数及以下参数。
源地址	选择匹配的源主机地址、地址范围或子网对象。
目的地址	选择匹配的目的地主机地址、地址范围或子网对象。
源端口	源端口或端口范围，只有“IP 协议类型”处选择了“TCP”或“UDP”时，才需要设置该参数。
目的端口	目的端口或端口范围，只有“IP 协议类型”处选择了“TCP”或“UDP”时，才需要设置该参数。 说明： 如果是允许访问某些目的端口，则如果端口为连续的，可以在目的端口处设定范围，否则需要对每一个端口设定相应的报文阻断策略。如果端口为唯一端口号，则要将起始和终止端口号设定为同一个值。

说明

-
- ✧ 如果定义阻断策略时同时输入了源 MAC 地址和源 IP 地址选项，则只有主机的 MAC 地址和 IP 地址均匹配此条件时，此规则才会生效。
-

c) 设置完成后，点击“确定”使此规则生效。点击“取消”放弃规则添加。

3) 修改策略属性

对于已经添加的阻断策略，管理员可以点击“操作”一列对应的“修改”图标修改该策略。

4) 删除策略

点击“操作”一列对应的“删除”图标，可以将策略从列表中删除。点击“清空”，则管理员可以一次性清除所有的阻断策略（不包括默认规则），便于重新配置。

5) 更改策略的匹配顺序。

安全设备接收到报文后，将顺序匹配阻断策略表中所设定的策略。一旦寻找到匹配的策略，则按照该策略所规定的操作（允许或拒绝）处理该报文。如果不存在可匹配的阻断策略，则会依据默认规则对该报文进行处理。所以策略的顺序将直接对报文转发速率产生影响。

阻断策略											
+ 添加 清空										总计: 2	
ID	控制	二层协议	源MAC	目的MAC	三层协议	源IP	目的IP	源端口	目的端口	区域	操作
当前默认规则为: 允许通过不记录日志											
8306	✓	0800			0					area_eth0	否
8307	✓	0800			0					area_eth1	否

点击操作栏中的“”图标，所有操作图标将显示出来，如下图所示。

阻断策略											
+ 添加 清空										总计: 2	
ID	控制	二层协议	源MAC	目的MAC	三层协议	源IP	目的IP	源端口	目的端口	区域	操作
当前默认规则为: 允许通过不记录日志											
8306	✓	0800			0					area_eth0	否
8307	✓	0800			0					area_eth1	否

如上图红框所示，点击某策略“操作”一栏的移动图标，则弹出移动窗口，可以更改策略的位置，如下图所示。



用户可以选择移动的参考 ID 以及位置（之前或之后），点击“确定”完成策略移动。或点击“取消”放弃策略移动。

9.2 访问控制规则

访问控制规则对报文实现基于内容的过滤方式，不仅能够检测报文的网络层和传输层信息，还能够检测报文的应用层内容。网络卫士安全网关接收到一个报文时，检测报文的源和目的区域、源 VLAN、源和目的地址、服务等，按照一定顺序检测访问控制规则表中是否有匹配的规则。如果有，则按照策略所规定的操作处理该报文；否则，将根据目的区域的缺省属性处理该报文。

系统提供对 ACL 规则的分组管理功能，不同组之间的前后顺序和组内规则的排列顺序共同决定访问控制规则的匹配顺序。

ACL 规则分为权限为“收集”的规则和权限为“允许”或“禁止”的规则两种。访问控制规则的配置包括规则组添加、规则管理、规则添加等内容。

说明

- ✧ 要实现对 GRE over IPSEC 流量进行访问控制，管理员首先要自定义一个属性，然后绑定该属性在 gre 口上，在要控制的区域内也添加该属性即可实现。

9.2.1 查看规则

- 1) 选择 防火墙 > 访问控制，进入访问控制规则定义界面。

访问控制						
目的区域	所有区域	策略组	所有组	高级搜索	☐	显示策略统计
+ 添加组		+ 添加策略		总计: 2 每页: 30条		
ID	控制	源	目的	服务	选项	操作
8261	✓	区域: area_eth1	区域: area_eth0	HTTP		 
8262	✓		区域: area_eth0	HTTPS		 
⏪ ⏩ 1 ⏪ ⏩ 转到 /1 Go						

表中“ID”为每项规则的编号，在移动规则顺序时将会使用。“控制”中的图标“√”和“×”，分别表示该项规则的访问权限是允许或拒绝；图标“”表示该规则仅用于收集符合条件的数据报文通过设备的情况，这样的收集策略通常位于策略列表的最后，并且不可移动到其他类型的策略之前。整条规则背景色为白色或浅蓝色时表示该规则为启用状态，背景色为灰色时表示该规则未启用。点击“操作”栏的“启用”或“禁用”图标可以启用或禁用该规则。

2) 当 ACL 规则较多时，管理员可以在“每页”处选择每页只显示前 10 条、20 条和 30 条规则。

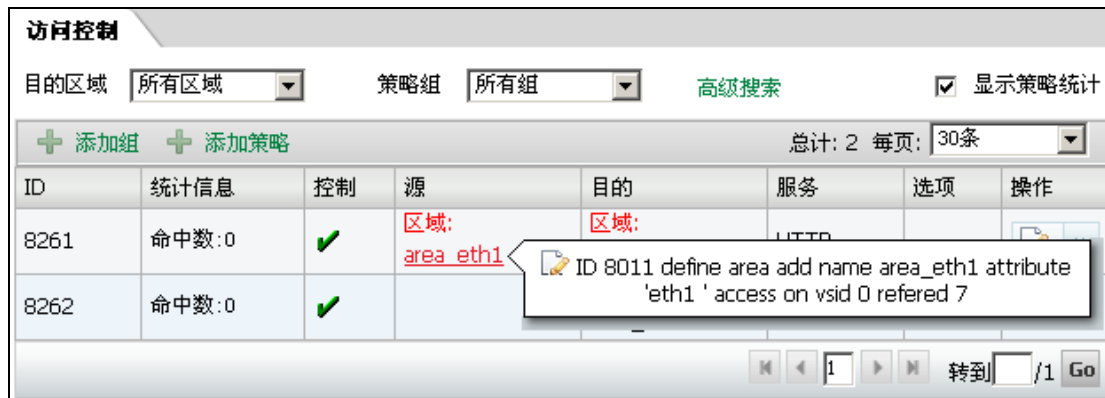
3) 默认情况下，将鼠标停留在规则 ID 号下方，管理员可以查看到当前该规则的匹配情况。如果在 ACL 规则中开启了“流量统计开关”，则当“权限”为允许时，显示“当前连接数、允许连接数、阻断连接数、历史包数”；当“权限”为禁止时，显示“当前连接数、阻断连接数”。如果在策略中没有开启“流量统计开关”，则仅显示“命中数”。如下图所示。



当勾选“显示策略统计”时，界面直接显示所有策略的匹配情况，如下图所示。



4) 将鼠标停留在源、目的、服务、时间等资源处，可以查看该资源的详细内容，如下图所示。



9.2.2 查询规则

网络卫士安全网关提供规则快速查询功能。当设备中的规则较多时，管理员在右侧页面中“目的区域”处选择要查询的规则的目的区域，并在“策略组”处选择所属的组，则符合条件的 ACL 规则将显示在页面下方的列表中。

如果需要进行进一步的精确查询，可以点击右侧的“高级搜索”，如下图所示。



则弹出下图所示界面。



管理员可以按照 IP 地址和资源名称来查找相应的访问控制规则，查找完成后，符合条件的 ACL 规则将显示在主界面的 ACL 规则列表中。

➤ 按照 IP 地址查找 ACL 规则

界面如上图。如果“源地址”和“目的地址”同时设定搜索条件，则只有和源、目的的同时匹配的 ACL 规则才符合查询条件。如果只设定“源地址”或“目的地址”，则只要 ACL 规则的源或目的匹配，就符合查询条件。

例如在“目的地址”栏输入 192.168.83.225 查找策略时，则所有源地址对象为 any 以及目的地址对象包含该 IP 的访问控制规则均匹配该查询条件，查询结果如下图所示。

访问控制

目的区域 所有区域 策略组 所有组 高级搜索 ☐ 显示策略统计

+ 添加组 + 添加策略

总计: 2 每页: 30条

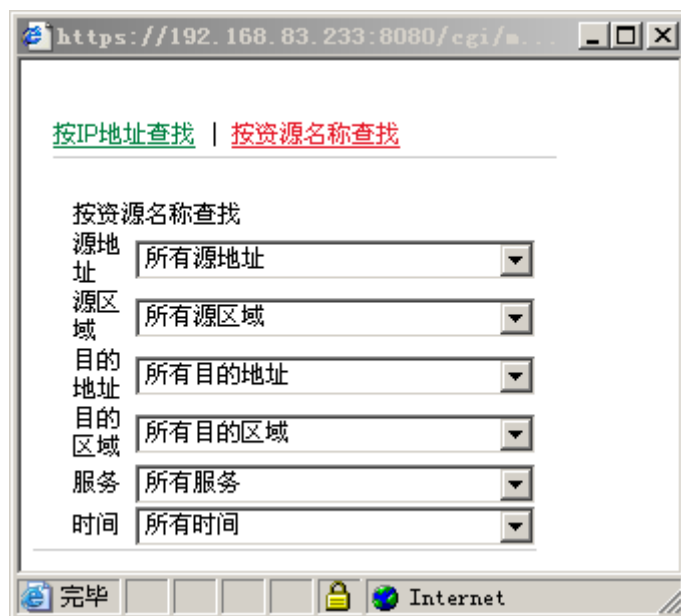
ID	控制	源	目的	服务	选项	操作
8261	✓	区域: area_eth1	区域: area_eth0	HTTP		 
8262	✓		区域: area_eth0	HTTPS		 

1

转到 /1 Go

➤ 按照资源名称查找 ACL 规则

界面如下图所示。



在上图界面中设定要查询的规则源地址、源区域、目的地址、目的区域、服务、时间中的一项或多项后，点击“查找”按钮，符合条件的结果将显示在主界面下方的访问控制规则列表中。

9.2.3 管理规则

网络卫士安全网关提供策略重叠检查功能，系统启动时为了保证效率，不做策略检查。用户可以在命令行下使用命令：**firewall enhancement switch overlap-exam on**开启“访问控制策略重叠检查”功能。开启后，在系统中不允许存在策略条件完全相同的访问控制策略。在管理员增加、修改ACL规则时检查是否有重复的策略，当管理员前后配置的两条策略相互矛盾时，系统也会有提示信息，进而可以有效避免用户的混乱配置。

说明

- ✧ 策略冲突检查功能，仅对启动该功能后的策略配置进行检查，不会对之前的配置进行冲突检查。

1) 启用或禁用规则

点击“操作”栏的对应图标可以启用或禁用该规则，如下图所示。



2) 修改规则

用户可以点击“操作”一列对应的修改图标，对现有规则进行编辑。

3) 插入规则

用户也可以点击“操作”一列对应的插入图标，在现有规则间插入一条新规则。

4) 复制规则

点击“操作”一列对应的复制图标，弹出访问控制规则设置界面，其参数与已有规则相同，管理员可以在界面中在原有规则的基础上再进行修改，使规则的设置更加方便。

5) 删除规则

点击“操作”栏的对应的删除图标可以删除该规则。点击“清空策略”，可以清除所有的访问控制规则，便于重新配置。

6) 调整规则顺序

访问控制规则执行**顺序匹配**原则，默认情况下，访问控制规则的排列顺序依据规则组的排列顺序、规则的排列顺序，以及规则中权限的类型共同决定，如下图所示。

访问控制

目的区域 所有区域 策略组 所有组 高级搜索 ☐ 显示策略统计

+ 添加组 + 添加策略 总计: 3 每页: 30条

ID	控制	源	目的	服务	选项	操作
research						 
market						 
默认组						-
8261		区域: area_eth1	区域: area_eth0	HTTP		 
8262			区域: area_eth0	HTTPS		 
8312		区域: area_eth2	区域: area_eth3	UDP	日志记录	 

  1   转到 / 1 Go

规则组的排列顺序决定了不同组成员的排列顺序，默认规则组排列在最后。

控制方式为“收集”的策略只能属于“默认规则组”，始终在列表的最后。

对于权限为“允许”或“禁止”的规则，管理员可以通过移动规则所属的规则组的顺序、移动同一类规则的顺序，来调整规则的排列顺序。

a) 移动规则组顺序

点击规则组对应的“移动”一列对应的图标，弹出界面如下图所示。



用户可以选择移动的参考规则组以及位置（之前或之后），点击“确定”完成规则组移动，或点击“取消”放弃移动。

b) 移动规则位置

点击规则对应的“移动”图标，弹出移动界面。



用户需要选择移动的参考 ID，并且选择移动位置（之前或之后），点击“确定”完成策略移动，或点击“取消”放弃策略移动。

9.2.4 添加规则组

对于定义的访问控制规则，系统提供对规则的分组管理功能，对规则分组管理将更改 ACL 规则的默认排列顺序，不同组之间的前后顺序和组内规则的排列顺序共同决定访问控制规则的匹配顺序。在添加访问控制规则时可以设置规则所属的组，安全网关系统内置的规则组为“默认组”，管理员可以添加新的规则组。

访问控制组的配置方法如下：

- 1) 选择 **防火墙 > 访问控制**，点击“添加组”，界面如下图。

在“名称”处输入访问规则组的名称。

- 2) 设置完成后，点击“确定”按钮完成规则组的添加，新添加的规则组没有成员，位于“默认组”之前，其余规则组之后。点击“取消”按钮放弃此次添加操作。

- 3) 对于手工添加的 ACL 组，点击“操作”一栏，选择“移动”图标可以移动 ACL 组的默认排列顺序（按照添加顺序排列），如下图所示。



用户可以选择移动的参考的 ACL 规则组的名称以及位置（之前或之后），点击“确定”完成策略组移动，或点击“取消”放弃策略组移动。

4) 插入规则组。

选择某手工添加的规则组，点击“操作”一列对应的插入图标，可以直接在该组的前面插入一条新的规则组。

5) 设置规则组成员。

对于规则组中的成员，可以在添加访问控制规则时指定，也可以通过修改规则属性来改变其所属的规则组。

不同组之间的前后顺序和组内规则的排列顺序共同决定访问控制规则的匹配顺序。

6) 删除规则组。

选择某手工添加的规则组，点击“操作”一列对应的删除图标，可以直接将该规则组删除。

9.2.5 添加规则

访问控制列表（Access Control List，ACL）的功能是过滤通过网络设备的特定数据包。ACL 通过一系列匹配条件对数据包进行分类，这些条件可以是数据包的来源区域、源地址、目的区域、目的地址、端口号等等，安全网关根据 ACL 中指定的条件来检测数据包，从而决定是转发还是丢弃该数据包。

1) 选择 **防火墙 > 访问控制**，进入访问控制规则定义界面。点击“添加策略”弹出窗口添加一条新的访问控制规则，如下图所示。

访问控制

添加访问控制策略

源

区域

任意

地址

任意

其它

☐

目的

区域

任意

地址

任意

其它

☐

服务

任意

动作

☒ 允许 ☐ 禁止 ☐ 收集

日志记录

☒ 不记录 ☐ 记录 ☐ 系统报警

连接选项

☐ 长连接

内容安全策略

无

高级

时间控制

无

IDS

无

IPS

无

QOS

总带宽限制

[默认单位: Kbps]

每主机带宽限制

[默认单位: Kbps]

高级

☐

DSCP

☐ 设置DSCP

☐ 设置COS

高级

☐

流量统计

☐ 开启

加入规则组

默认组

规则描述

确定

取消

参数说明如下表所示：

参数	说明
源	选择对象，设定发起连接的源应当匹配的条件。可以实现基于哪些条件对报文进行访问控制。如果不指定，表示任何源地址均匹配该规则。可设定的选项包括： 1) 区域：选择区域资源限定报文的来源区域。 2) 地址：选择已定义的地址资源对象，限定报文的源 IP 地址。 3) 角色：选择已定义的用户角色对象，限定发起连接的用户角色。 4) VLAN：对报文的源 VLAN 进行限定。 5) 端口：选择服务对象，限定源端口。

参数	说明
	说明： 1) 多个选项设定的条件之间是“与”的关系，数据包的源地址在匹配规则的时候必须都要匹配上选择的选项，规则才能生效。 2) 每一选项均可选择多个对象，多个对象之间是“或”的关系。只要满足其中一个对象即可。 3) 当没有设置地址对象时，默认表示任意地址。 4) 对通过 Topsec 认证客户端登录的普通用户和通过浏览器登录的 CGI 用户可以基于角色进行访问控制。对 VRC 用户需要在 VRC 管理中的开启“与防火墙联动”这一选项。对 SV 用户无法通过引用角色对象进行访问控制，只能通过创建相应分配地址的地址对象，再在访问控制中引用这个对象进行控制。
目的	选择对象，设定发起连接的目的应当匹配的条件。可以实现基于哪些条件对报文进行访问控制。当设定多项时，必须同时满足各个条件才匹配该规则。如果不指定，表示任何源地址均匹配该规则。可设定的选项包括： 1) 区域：选择区域资源限定报文的目的区域。 2) 地址：选择已定义的目的地址资源对象，限定报文的目的 IP 地址。由于安全网关会首先对报文进行目的 NAT 转换，然后再查询匹配的 ACL 规则，因此，在“选择目的地址”处管理员应当选择与 DNAT 转换后的真实 IP 地址匹配的地址对象。如果想对转换前的目的地址进行检测，则在此处不需要设置，需要在“其它”属性中设置“转换前的目的地址”项。 3) VLAN：对报文的目的 VLAN 进行限定。 4) 转换前地址：如果想对转换前的目的地址进行检测，则需要设定该选项。否则，只需设置“目的地址”即可。 5) 目的域名：选择 DNS 资源对象。则只要目的 IP 属于该 DNS 对象的 IP 地址池，报文就匹配 ACL 规则，安全网关将按照规则的权限对报文进行处理，从而实现基于域名的访问控制。 说明： 1) 多个选项设定的条件之间是“与”的关系，数据包的目的地址在匹配规则的时候必须都要匹配上选择的选项，规则才能生效。 2) 每一选项均可选择多个对象，多个对象之间是“或”的关系。只要满足其中一个对象即可。 3) 当没有设置地址对象时，默认表示任意地址。
服务	选择服务对象，对数据报文的协议和目的端口号进行限定。如果没有选择任何服务，则系统默认为不对协议和端口号进行限定。 说明： 如果用户需要指定的服务没有包含在服务列表中，可以通过添加自定义服务添加所需服务，具体操作请参见7.4.2 自定义服务。
动作	设置对于匹配规则的数据报文采取的操作。 1) 当选择“允许”或“禁止”时，对于匹配规则的数据报文，允许或禁止通过设备。

参数	说明
	2) 当选择“收集”时, 对于匹配规则的数据报文, 允许报文通过, 并对匹配该策略的信息进行记录, 无论该条策略是否做日志。管理员可以选择 防火墙 > 访问记录 , 查看匹配规则的报文, 具体请参见 9.3访问记录 。
日志记录	设置是否记录日志或报警。共有 3 个选项: 否(表示不记录日志或报警)、日志记录、系统报警。
连接选项	可以为普通连接, 也可以为长连接, 一般来说, 安全网关对通信空闲一定时间的连接将自动断开, 以提高安全性和释放通信资源, 但某些应用所建立的连接需要长时期保持, 即使处于空闲状态。例如 ATM 机器必须和处理中心的服务器一直保持着连接, 这个连接必须设置为长连接。
内容安全策略	选择已经设置的内容安全策略对象, 匹配到本条访问控制规则的数据包将根据对象中定义的策略对其进行处理。关于内容安全策略的设置请参见 9.6内容安全策略 。
时间控制	设置该访问控制规则生效的时间段。如果没有选择时间段对象则表示所有时间。时间对象定义请参见 7.3设置时间资源 。
IDS	选择已经设置的IDS规则对象, 匹配到本条访问控制规则的数据包将根据相应的IDS对象对其进行处理。关于IDS对象的设置请参见 14.3.1设置IDS规则 。
IPS	选择已经设置的 IPS 策略, 匹配到本条访问控制规则的数据包将根据 IPS 策略中定义的策略对其进行处理。关于 IPS 策略的设置请参见《TopGate 管理手册——IPS 配置》。
QoS	对符合 ACL 规则的数据流进行流量监管。有两种设置方法: 1) 通过简单的设置“总带宽限制”或“每主机带宽限制”。“总带宽限制”是指所有匹配规则的源 IP 地址的总限制带宽, “每主机带宽限制”是指匹配规则的每一个 IP 地址单独享有的限制带宽。只设置“总带宽限制”时添加“策略独享”类 QoS 策略; 只设置“每主机带宽限制”时添加“独享”类 QoS 策略; 同时配置“总带宽限制”和“每主机带宽限制”时, 则只能添加“受控”类 QoS 策略。 2) 通过勾选“高级”选项, 选择设定的“QoS 对象”来设置流量策略。如果所引用的流量策略中设置了保证带宽, 则必须在 ACL 规则中设置数据出接口的区域, 也就是说: 如果在 QoS 对象中设置“上行”策略, 则 ACL 规则必须设置“目的区域”; 如果设置“下行”策略, 则 ACL 规则必须设置“源区域”。
DSCP	网络卫士安全网关可以根据 ACL 规则, 以及 IP 包头的 DSCP 值识别数据包, 并在数据包的 IP 层和二层上分别标记新的 DSCP 值和 COS 值, 便于下游的网络设备根据优先级对报文进行流量控制。 说明: 1) DSCP 字段位于 IP 报文头部 TOS 字段的前 6 位, 值有 64 个(0-63), 0 为最低优先级, 63 为最高优先级。 2) COS 值又称 802.1P 优先级, 为带有 VLAN 标签的以太网数据包

参数	说明
	的 COS 字段，占用 3 个 bit，值有 8 个（0-7），0 为最低优先级，7 为最高优先级。只有当数据报文的出接口为 Trunk 口时 COS 值才有效。 3)一般情况下，仅根据 ACL 规则判断是否对报文的优先级进行标记，不检测报文的 DSCP 值。当需要进一步限定报文的 DSCP 值时，需要在“高级”选项中勾选“匹配原始 DSCP 值”，并设置匹配条件，此时报文不仅要匹配 ACL 规则，而且报文的 DSCP 字段必须匹配“原始 DSCP 值”，否则不对报文的优先级进行重新标记。
流量统计	设置是否开启流量统计开关，开启后系统将对匹配规则的流量进行统计。管理员可以将鼠标置于策略 ID 上查看流量统计结果。如果在策略中没有开启“流量统计开关”，则仅能查看“命中数”。 说明： 如果在策略中开启了“流量统计开关”，则当策略为允许时，可以查看“当前连接数、允许连接数、阻断连接数、历史包数”；当策略为禁止时，仅能查看“当前连接数”和“阻断连接数”。
加入规则组	设置该规则所属的规则组。可选项为“默认组”，或管理员添加的规则组。规则组设置请参见 9.2.4添加规则组。 说明： 当“访问权限”设置为“收集”时，规则组只能选择“默认组”。
规则描述	输入对该 ACL 规则的必要描述信息。

点击“确定”完成该条访问控制规则的设定。点击“取消”放弃该规则添加。

使用小技巧

技巧 1:

图中“编辑”按钮将弹出选择资源窗口，用于设定规则的匹配条件。

技巧 2:

管理员可以在界面中直接添加资源对象。

9.3 访问记录

当“访问记录”开关为“开启”状态时（默认开启），如果通过设备的报文匹配访问权限类型为“收集”的访问控制规则，网络卫士安全网关系统将记录其连接信息，管理员可以查看到相关的访问记录。具体方法为：

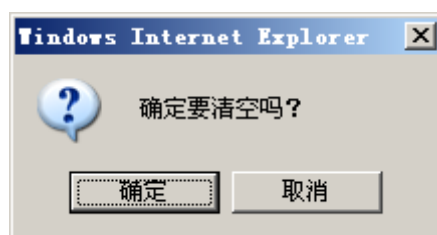
1) 选择 **防火墙 > 访问记录**，在右侧页面内显示匹配ACL记录规则的连接信息，如下图所示。

访问记录						
访问收集		开启	停止			
刷新页面		清空记录		总计: 1		
源地址	目的地址	协议	目的端口	状态	生成策略	
192.168.83.220	172.16.1.2	UDP	22105	未匹配		

在上图中，所有记录默认按照源地址从小到大顺序排列。点击标题栏对应的图标“”，可以实现记录按照该列标题进行排列。例如点击“源地址”一栏对应的图标，则可实现所有记录按照源地址倒序排列。再次点击图标，实现正序排列。

2) 点击“刷新页面”，则管理员可以查看到最新的记录信息。

3) 点击“清空记录”，则弹出如下图确认窗口，点击“确定”按钮，可以将页面所有的记录信息一次清空。



4) 根据记录信息生成 ACL 策略。

点击记录对应的“生成策略”一列对应图标，弹出生成策略窗口，如下图所示。管理员可以直接生成 ACL 策略。

生成策略

源地址：

名称

☒ 主机

☐ 范围 到

☐ 子网 掩码

目的地址：

名称

☒ 主机

☐ 范围 到

☐ 子网 掩码

服务：

名称

协议

端口 到

访问权限：☒ 允许 ☐ 拒绝

确定 取消

完成 Internet 100%

选择 **防火墙 > 访问控制**，可以查看到已经在默认组中添加了相应的ACL规则，如下图所示。

访问控制

目的区域 所有区域 策略组 所有组 高级搜索

+ 添加组 + 添加策略

总计: 6 每页: 30条

ID	控制	源	目的	服务	选项	操作
kkk						
111						
默认组						-
8102	✓	区域: area_eth2 地址: 配置人员	区域: area_eth1		QOS: [share_out]	
8105	✓	区域: pptp_area	地址: 192.168.83.225		QOS: [总带宽限制:;每主机带宽限制:200KBps]	
8128	✓	地址: 192.168.83.220	地址: 172.16.1.2	UDP_22105		
8034		区域: area_eth0	区域: adsl_area 地址: any		QOS: [总带宽限制:600KBps;每主机带宽限制:]	
8123		区域: area_eth0				

1

转到 /1 Go

5) 点击“停止”按钮，系统将停止记录与类型为“收集”的 ACL 规则相匹配的连接信息。点击“启用”按钮可以再次启用该功能。

9.4 地址转换

9.4.1 基本概念

所谓网络地址转换，是将 IP 数据报头中的 IP 地址转换为另一个 IP 地址的过程。网络卫士安全网关提供以下几种地址转换方式：

- 源地址转换（SNAT）。可以实现具有私有地址的用户对公网的访问。
- 目的地址转换（DNAT）。可以实现公网上的用户对位于内网的具有私有地址的服务器的访问。
- 双向地址转换（双向 NAT）。可以实现一个内网 IP 地址到另一个内网 IP 地址的访问。
- 不做转换（NoNAT）。一般用于定义源 NAT 和双向 NAT 规则的特例，此时 NoNAT 规则需要置于匹配范围较大的 NAT 规则前面。

在网络卫士安全网关上，通过选择已经定义的资源对象来设定进行 NAT 转换的数据包应当满足的匹配条件。如果在某一个选项处设置了多个条件，则必须同时满足这些条件才认为匹配该规则。例如在“源区域”处选择 “area_eth0”，源地址选择“172.16.1.2”对象，那么，只有发起连接的源属于区域 area_eth0，同时，源 IP 地址包含在 172.16.1.2 对象中时，对报文才进行地址转换。

网络卫士安全网关中定义的所有地址转换规则都按一定顺序存储在一张规则表中。当数据包通过设备时，首先检测 DNAT 规则，然后检测访问控制规则，最后再检测 SNAT、双向 NAT 和 NoNAT 规则。每次检测时都按照规则的排列顺序逐一与数据包匹配，一旦存在一条匹配的地址转换规则，网络卫士安全网关将停止检索，并按所定义的规则处理数据包。因此，匹配条件严格的规则应当置于条件宽松的规则之前。

9.4.2 查看 NAT 规则

配置 NAT 规则步骤为：

- 1) 在左侧导航菜单选择 **防火墙 > 地址转换**，进入地址转换规则列表界面，如下图所示。



整条规则背景色为白色时表示该规则为启用状态，背景色为灰色时表示该规则未启用。只有启用状态的规则才会对数据报文进行检测。

列表中各个字段的含义说明如下表：

参数	说明
ID	每项规则的编号，在移动规则顺序时将会使用。
类型	显示地址转换方式：源转换、目的转换、双向转换和不作转换。
源	显示该策略的源匹配条件，可能包含源地址、源 VLAN、源区域、源端口中的一项或多项。

参数	说明
目的	显示该策略的目的匹配条件。可能包含目的地址、目的 VLAN、目的区域中的一项或多项。
服务	显示策略的服务匹配对象。
转换	显示对匹配报文的地址进行的转换。
操作	显示管理员可以对该策略进行的所有操作图标，点击图标即可实现相应操作。包括： 1) 修改图标：点击图标，可以修改规则属性。 2) 复制图标：点击图标，可以复制一条参数相同的新规则，管理员可以在界面中原有规则的基础上再进行修改，使规则的设置更加方便。 3) 移动图标：点击图标，可以在列表中移动策略位置。 4) 插入策略：点击图标，可以将新添加的 NAT 规则插入到某项规则之前。 5) 启用/禁用策略：点击图标可以启用或禁用该规则。 6) 删除策略：点击图标，可以从列表中删除该规则。

2) 查看规则

- a) 将鼠标停留在规则 ID 号下方，管理员可以查看到当前该规则的匹配情况。
- b) 将鼠标停留在源、目的、服务、时间等资源处，可以查看该资源的详细内容。
- c) 当规则较多时，管理员可以在“每页”处选择每页只显示前 10 条、20 条和 30 条规则，然后点击逐个页面进行查看。
- d) 当勾选“显示策略统计”时，界面直接显示所有策略的匹配情况。

3) 输入查询条件查找规则

在右侧页面中“目的区域”处选择要查询的规则的目的区域，则符合条件的 NAT 规则将显示在页面下方的列表中。

如果需要进行进一步的精确查询，可以点击右侧的“高级搜索”，则弹出下图所示界面。



在上图界面中设定要查询的规则源地址、源区域、目的地址、目的区域、服务中的一项或多项后，点击“查找”按钮，符合条件的结果将显示在主界面下方的列表中。

9.4.3 添加 NAT 规则

管理员可以点击“添加”按钮添加一条新的 NAT 规则，新规则位于规则表的末端。

管理员也可以直接点击某条规则所在行的“插入”图标，可以直接将新添加的规则插入该规则之前。如果新添加的规则与已有规则参数类似，管理员可以点击已有规则对应的复制图标，则添加规则界面中已经设置了与已有规则相同的参数，管理员可以在界面中在原有规则的基础上进行修改，使规则的设置更加方便。

1) 点击“添加”按钮，添加界面如下图所示。

添加地址转换

模式

源转换

源

地址

任意

✎

☐ 其它

目的

地址

任意

✎

☐ 其它

服务

任意

✎

源地址转换为

---不做转换---

▼

源端口不做转换

☐ [源端口固定]

规则描述

确定

取消

参数说明如下表所示：

参数	说明
模式	选择地址转换方式：可选项为源转换、目的转换、双向转换和不作转换。
源	配置数据报文的源应当匹配的条件，可以设定报文的源地址、源 VLAN、源区域、源端口中的一项或多项应当匹配的条件。点击“编辑”按钮，弹出选择对象窗口，管理员可以选择已经定义的资源对象。
目的	配置数据报文的目的应当匹配的条件。可以限定报文的目的地址、目的 VLAN、目的区域中的一项或多项。
服务	选择匹配的服务对象，可以选择一个或多个。
源地址转换为	只有当选择“源转换”和“双向地址转换”方式时需要设置该参数。选择转换后的主机地址、地址范围对象或属性对象。 说明： 1) 当选择主机地址对象时，表示即将源地址固定映射为某一合法 IP 地址； 2) 当选择地址范围对象时，将源地址动态映射为某一网段或某一地址范围的地址。 3) 选择属性对象时，将源地址转换为具有该属性的物理接口的地址（默认映射为端口的主地址）。因此要求属性对象必须

参数	说明
	与物理接口绑定，具体设置请参见 6.2.1物理接口 。
源端口不作转换	当选择“源转换”和“双向地址转换”方式时需要设置该参数。系统默认情况下，在源地址转换同时也会转换源端口。如果勾选该选项时，表示数据包在经过安全网关时将固定源端口而不对源端口进行随机转换。
目的地址转换为	当选择“目的转换”和“双向地址转换”方式时需要设置该参数。选择转换后的目的地址，可以选择具体的主机地址，或者选择已设定的负载均衡组。关于负载均衡组的设定请参见 16.4.2定义负载均衡组 。
目的端口转换为	当选择“目的转换”和“双向地址转换”方式时需要设置该参数。设置转换后的服务端口，可以选择系统预定义的服务或用户自定义的服务。
启用规则	勾选后该规则才会生效。默认为启用状态。
规则描述	可选项，输入必要的描述字符串。

小技巧：

管理员可以通过点击“编辑”按钮，在弹出的窗口中选择资源对象，如下图所示：



当资源对象较多时，界面中对象右侧的排序按钮用于按照 ASCII 码的正序排列和倒序排列下面列表框中的对象。点击“查找”图标按钮，左侧弹出文本框，管理员可以输入查询条件，则含有该字符的对象名称将被选中，可以方便用户按序查找项目。

当列表中没有需要的资源对象时，管理员可以在界面右上方的“定义对象”处选择添加的资源类型，来直接添加资源对象。

2) 所有参数设定完成后，点击“确定”按钮，新添加的规则会显示在“地址转换”页面中的最后一条。

9.4.4 改变 NAT 规则的位置

当列表中有多个规则匹配数据包时，排列在列表中前面的规则将首先进行匹配，之后停止规则检查，实际上排列在后面的规则将失效。因此，匹配条件严格的规则应当置于条件宽松的规则之前。

管理员可以在列表中移动规则的位置，从而改变 NAT 规则的匹配顺序。步骤为：

1) 点击规则后的“操作”一栏“移动”图标，弹出移动界面如下图所示。



在第一个下拉框中选择参考位置规则 ID 号，第二个下拉框中则是选择将当前策略移动到参考策略“之前”或“之后”。

2) 点击“确定”按钮，完成 NAT 规则的移动。

9.5 IP/MAC 地址绑定

IP/MAC 绑定技术是将主机的 IP 地址和网卡的硬件地址绑定起来，目的是为了防止 IP 欺骗、地址伪装，主要用于绑定一些重要管理员 IP 和特权 IP。当某个 IP 通过安全网

关访问时，安全网关要检查发出这个 IP 广播包的 MAC 地址，并与安全网关上的 MAC 规则相比较，如果相符就允许通过；否则不允许通过安全网关。此种技术特别适用于防止外部用户假冒内部地址穿过安全网关来访问内部网络。

添加 IP/MAC 地址绑定策略有两种方法：

- (1) 手工添加策略；
- (2) 通过 ARP 探测添加策略：利用发送 ARP 包来检测网络中处于活动状态的主机，实现 IP 地址和 MAC 地址的自动搜集，从而实现批量 IP 地址和 MAC 地址绑定。每次最多能探测 255 个主机地址。

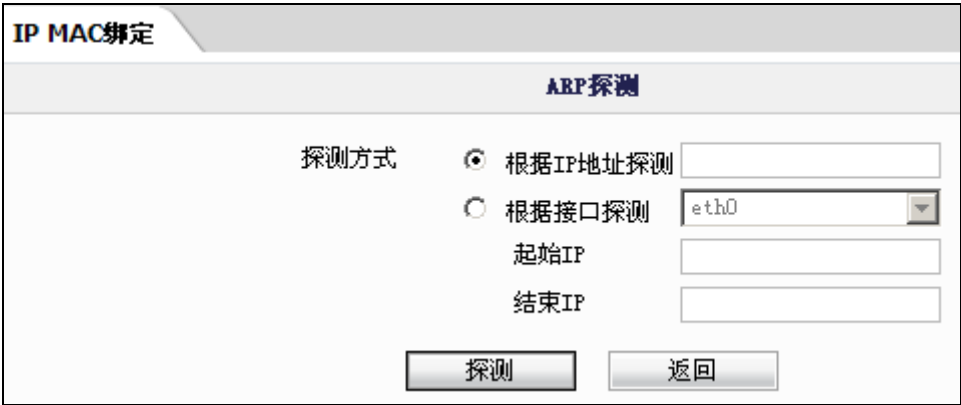
设置 IP/MAC 绑定策略的操作如下：

- 1) 选择 **防火墙 > IP/MAC绑定**，右侧界面显示已有的配置，如下图所示。



- 2) 通过 ARP 探测添加绑定策略

- a) 点击“探测”，界面如下图所示。



参数说明如下表所示：

参数	说明
根据 IP 地址探测	输入 IP 地址字符串。不能输入广播地址或组播地址，否则系统会提示错误并返回。
根据接口探测	选择物理接口、VLAN 虚接口或子接口名，如“eth0”，如果接口不存在或者该接口没有指定 IP，则系统提示错误并返回。

参数	说明
起始 IP	输入探测的起始 IP 地址，该地址必须在接口所属的子网内，而且要和“结束 IP”在同一个子网内。 说明： 如果起末 IP 地址不在该接口子网内、起末 IP 不属于同一个子网或者要检测的 IP 数大于最大探测数量 255，则系统提示错误并返回。
结束 IP	输入探测的结束 IP 地址。

b) 点击“探测”发送 ARP 包，则下面的列表中将显示探测到的 IP/MAC 地址对应表。如下图所示。

IP MAC绑定

ARP探测

探测方式

☐ 根据IP地址探测
☒ 根据接口探测

起始IP

结束IP

eth0

探测 返回

探测结果

IP地址	MAC地址	状态	接口	全选 ☐
192.168.83.224	00:50:04:c3:b0:31	正常	eth0	☐
192.168.83.3	00:0d:60:77:0a:4f	正常	eth0	☐
192.168.83.235	00:13:d4:0d:30:69	正常	eth0	☐
192.168.83.1	00:13:32:05:11:0a	正常	eth0	☐

绑定

c) 点击“全选”则直接选定列表中的所有探测到的对象。也可选择部分需要绑定的 IP/MAC 地址对应项目，例如上图，点击“绑定”，则完成 IP/MAC 地址的绑定操作，结果如下图所示。

IP MAC绑定			
探测 添加 清空			总计: 5
主机	IP	MAC	操作
192.168.83.234	192.168.83.234	00:11:d8:a8:9a:22	
192.168.83.224	192.168.83.224	00:50:04:c3:b0:31	
192.168.83.3	192.168.83.3	00:0d:60:77:0a:4f	
192.168.83.235	192.168.83.235	00:13:d4:0d:30:69	
192.168.83.1	192.168.83.1	00:13:32:05:11:0a	

3) 手工添加 IP/MAC 地址绑定。

点击“添加”，系统出现添加配置页面，如下图所示。

IP MAC绑定

添加配置

主机

webserver

MAC地址

[格式如 AA:BB:CC:DD:EE:FF]

确定

取消

参数说明如下表所示：

参数	说明
主机	选择已定义的主机地址资源，关于主机地址资源的设置请参见 7.1.1 设置主机资源 。
MAC 地址	输入与主机地址资源绑定的 MAC 地址。

点击“确定”完成对主机地址资源和 MAC 地址绑定策略的配置。

4) 点击“修改”或“删除”图标可以修改或删除已添加的配置。点击“清空”按钮可以一次性删除所有的绑定策略。

9.6 内容安全策略

内容保护表用于配置对应用层协议数据的处理策略，网络卫士安全网关支持的应用层协议包括 HTTP、FTP、SMTP、POP3、IMAP、DNS、TELNET 和 RSH 等协议，以及各种即时通讯协议。

- [HTTP过滤](#)：对HTTP协议数据配置网页内容过滤和网页重定向服务。
- [FTP过滤](#)：对FTP协议数据配置文件名称和权限过滤、FTP操作命令过滤。
- [WEB过滤](#)：设置拒绝用户访问的恶意网站。
- [邮件过滤](#)：对POP3、SMTP以及IMAP协议数据配置主题、内容、附件中的文件名以及收件人和发件人的名称进行过滤。
- [防病毒](#)：对HTTP，FTP，IMAP，POP3 与SMTP等协议，以及应用程序识别策略配置反病毒保护。
- [反垃圾邮件](#)：配置反垃圾邮件过滤服务。
- [应用程序识别](#)：对即时通讯软件（如：MSN、QQ、网易泡泡、新浪UC、Yahoo! Messenger、阿里旺旺、迅雷和SKYPE等）配置过滤、带宽控制及访问控制。
- [其他协议过滤](#)：对通过RSH、TELNET传输的命令进行关键字过滤，对通过设备的DNS查询请求进行域名过滤。
- [记录日志](#)：配置是否在系统日志中记录各个协议过滤的情况。

管理员可以根据实际需要，在内容安全策略中设置启用或禁用某些协议或功能。

需要特别注意的是：

（1）配置内容安全策略后，必须在访问控制规则中引用该策略，才可以实现对应用层数据的过滤功能。对匹配ACL规则的网络连接，将首先根据应用端口绑定策略，根据五元组中的目的端口和协议类型确定应用层协议类型（请参见 [10.4应用端口绑定](#)）；然后按照所引用的内容安全策略的配置，对数据采取相应协议对应的处理方案。因此，即使在内容保护表中选择了很多选项，到达的会话只做五元组命中的过滤，比如即使在内容安全策略中定义了HTTP协议以外的其他协议的策略，一个HTTP会话也不会去做HTTP以外的过滤检查。

（2）对于同一个协议，可以配置多种过滤方式，则系统将按照一定的顺序进行检查，如果会话命中靠前的过滤功能，那么后面的过滤将不执行。

对于 HTTP 协议，如果在内容保护表中同时配置了 HTTP 内容过滤、URL 过滤、Web 过滤和病毒过滤的策略，则检查顺序为：HTTP 内容过滤->URL 过滤->Webfilter->病毒过滤。

对于邮件类协议（POP3、SMTP 和 IMAP），如果在内容安全策略中同时配置了邮件过滤、反垃圾邮件和防病毒过滤策略，则检查顺序为邮件过滤->反垃圾邮件->防病毒过滤。

对于 FTP 协议，如果在内容安全策略中同时配置了 FTP 过滤和防病毒过滤策略，则检查顺序为 FTP 过滤->防病毒过滤。

内容安全策略的配置步骤为：

1) 选择 **防火墙 > 内容安全策略**，界面如下图所示。

内容安全策略			
 添加		 清空	总计: 1
名称	保护内容	描述信息	操作
doc_test	反垃圾邮件 防病毒		 

点击“操作”一列的修改图标可以修改策略。

点击“操作”一列的删除图标可以删除对应的策略；点击“清空”可以一次性删除所有未被规则引用的安全策略。

2) 点击“添加”，可以添加内容安全策略。界面如下图所示。



The image shows a configuration window titled "内容安全策略" (Content Security Strategy). It contains a "策略名称" (Strategy Name) field with a red asterisk indicating it is required, and a "注释信息" (Comment Information) text area with a character limit of 63. Below these fields is a list of filter categories: HTTP过滤, FTP过滤, WEB过滤, 邮件过滤, 防病毒, 反垃圾邮件, 应用程序识别, 其他协议过滤, and 记录日志. At the bottom are "确定" (OK) and "取消" (Cancel) buttons.

在“策略名称”处输入对象名称，必须小于 32 个字符。一个汉字占用 2 个字符。

禁止输入“none/NONE/None”关键字作为过滤策略的名称。

a) 设定 HTTP 过滤策略：

可以同时设置内容过滤策略和重定向策略，系统先进行重定向，再进行 HTTP 过滤。

内容过滤：依据页面 URL、关键字和脚本等特征，对 HTTP 访问进行过滤，以便控制用户访问敏感网页，并禁止通过 HTTP 脚本或 Java 程序传播网络病毒。系统将首先过滤网页的内容，然后再对 URL 进行过滤。

HTTP 重定向：当用户在指定时间段内首次访问某 WEB 服务器时，将其重定向到指定的 WEB 页面。

设置界面如下图：

HTTP过滤	
内容过滤	
URL过滤	未选择
URL最大长度	[0-4096, 0为不限制]
网页内容过滤	未选择
http头过滤	未选择
ActiveX过滤	☐
Applet过滤	☐
Script过滤	☐
识别伪装HTTP连接	允许
登录标题替换	未选择
重定向	
重定向地址(最多127个字符)	
	周期: [0-604800秒]

参数说明如下表：

参数	说明
URL 过滤	选择已定义的 URL 过滤对象，设置对哪些 URL 地址进行过滤。 说明： 当传输的 HTTP 协议的 URL 地址匹配选中的 URL 对象时，根据 URL 对象的权限对数据包进行处理；否则，处理权限与关键字的权限相反。
URL 最大长度	设置 URL 地址的长度的最大值，对于通过前面检测的用户，如果 URL 的最大长度超过此处设定的数值，则拒绝通过设备。设为 0 时不限制，范围为 0—4096，单位为字节。
网页内容过滤	选择已定义的HTTP协议的关键字对象，设置对对HTTP页面中的哪些关键字定义的内容进行过滤。关键字定义请参见 10.2.2内容过滤 。 说明： 1. 当传输的 HTTP 协议的网页内容包含设置的关键字对象时，根据关键字的权限对数据包进行处理；否则，处理权限与关键字的权限相反。 2. 如果之前没有定义关键字对象，可以在下拉列表框中选择“新建关键字”，添加新的关键字对象。
HTTP 头过滤	可以设置对HTTP协议头中的哪些关键字定义的Header进行过滤。关键字定义请参见 10.2.2内容过滤 。
ActiveX 过滤	设置是否允许在 HTTP 协议中传输 ActiveX 控件。默认允许，勾选后禁止传输。
Applet 过滤	设置是否允许在 HTTP 协议中传输 Applet 控件。默认允许，勾选后禁止传输。
Script 过滤	设置是否允许在 HTTP 协议中传输 Script 控件。默认允许，勾选后禁止传输。
识别伪装 HTTP 连接	设置是否允许伪装 HTTP 的非法报文（即 80 端口非 HTTP 报文）通过设备。默认为“允许”，当设置为“禁止”时将拦截伪装 HTTP

参数	说明
	的非法报文。
登录标题替换	选择登录标题关键字对象，当连接匹配 ACL 规则时，将用选择的关键字对象替换服务器返回的 Banner 信息。 说明： 如果之前没有定义登录标题对象，可以选择“新建关键字”添加登录标题对象。
重定向地址	指当用户首次访问某 WEB 服务器时，符合该策略的 HTTP 访问被重定向到的 URL 地址。用户关闭重定向页面后，在“周期”设定的时间内可以正常访问，超过这段时间后就会重新跳转到重定向页面。 说明： 1. 重定向地址必须设置为完整的 URL 地址，最多不能超过 127 个字符。 2. 重定向周期单位为秒，取值范围：0-604800。

b) 设定 FTP 过滤策略：

通过控制文件的名称和权限、过滤 FTP 操作的命令来实现 FTP 过滤，保障网络主机的安全。

设置界面如下图：

▼ FTP过滤

文件名控制	未选择						
允许上传	☒						
允许下载	☒						
登录标题替换	未选择						
命令过滤							
上传	☐	下载	☐	追加	☐	删除文件	☐
重命名	☐	列表	☐	创建目录	☐	删除目录	☐

参数说明如下表：

参数	说明
文件名控制	选择已定义的 FTP 协议关键字，设置对哪些通过 FTP 传输的文件名进行过滤。 说明： 对于匹配 ACL 规则的所有连接，当传输的 FTP 协议的文件名匹配选中的对象时，根据对象的权限对数据包进行处理；否则，处理权限与关键字的权限相反。
允许上传	选中“允许上传”，表示不匹配文件名时，FTP 策略默认允许文件的上传；
允许下载	选中“允许下载”，表示不匹配文件名时，表示 FTP 策略默认允许

参数	说明
	文件的下载。
登录标题替换	选择登录标题关键字对象，设置用来替换服务器返回的 Banner 信息的登录标题。 说明： 如果之前没有定义登录标题对象，可以选择“新建关键字”添加登录标题对象。
命令过滤	选择允许传输的 FTP 命令。 说明： 上传：包含 put,mput,send 命令； 下载：包含 get,mget,recv 命令； 追加：包含 append 命令； 删除：包含 delete,mdelete 命令； 重命名：指 rename 命令； 列表：包含 ls,dir,mls,mdir,mdelete,mget 命令； 创建目录：指 mkdir 命令； 删除目录：指 rmdir 命令；

c) WEB 过滤：

设置拒绝用户访问的网站。

每一类网站中所包含的具体网站的URL地址由天融信公司来维护，管理员可以通过手动更新或自动更新方式进行实时更新网站名单列表，具体请参见 [4.3.6.4更新URL库](#)。

具体参数设置界面如下图：

WEB过滤	
启用警告页面发送	☒
启用恶意网站允许跳过	☐
类型	阻断
▶ 天融信恶意网站过滤	☐
▶ 违反国家法规与政策	☐
▶ 潜在不安全的	☐
▶ 潜在浪费带宽	☐
▶ 大众兴趣	☐
▶ 文化、时评、聊天与论坛	☐
▶ 行业分类	☐
▶ 计算机技术相关	☐
▶ 其它分类	☐

参数说明如下表所示：

参数	说明
启用警告页面发送	设置违反 Webfilter 策略时系统是否显示警告页面。
启用恶意网站允许跳过	管理员可以根据需要设置对“天融信恶意网站”中的挂马网站直接放行。 说明： 该选项只有当“天融信恶意网站”勾选“阻断”时才有效。
类型	选择将哪些网站作为恶意网站进行过滤。列表中显示网站的分类信息，点击左侧的蓝色箭头按钮，可以查看每一类网站的详细分类信息。可以勾选大的分类标题，则该类网站的所有子类网站均被作为恶意网站。也可以只勾选小的分类网站。如果不勾选，则允许访问该类网站。

d) 邮件过滤：

对使用 SMTP、POP3 和 IMAP 协议发送的邮件的主题、内容、附件中的文件名以及收件人和发件人的名称进行过滤。参数设置界面如下图：

▼ 邮件过滤				
	SMTP	POP3	IMAP	选项
发件人过滤	☐	☐	☐	未选择 ▼
收件人过滤	☐	☐	☐	未选择 ▼
主题过滤	☐	☐	☐	未选择 ▼
附件过滤	☐	☐	☐	未选择 ▼
邮件正文过滤	☐	☐	☐	未选择 ▼
登录标题替换	☐	☐	☐	未选择 ▼
转发不符合安全规则的邮件	关闭 ▼	关闭 ▼		

参数说明如下表：

参数	说明
发件人过滤	选择已经添加的 MAIL 协议关键字，设置发件人应匹配的关键字。匹配关键字时，将对邮件按照关键字的权限处理邮件，否则，按照相反的权限进行处理。
收件人过滤	选择已经添加的 MAIL 协议关键字，设置收件人应匹配的关键字。匹配关键字时，将对邮件按照关键字的权限处理邮件，否则，按照相反的权限进行处理。
主题过滤	选择已经添加的 MAIL 协议关键字，设置邮件主题应匹配的关键字。匹配关键字时，将对邮件按照关键字的权限处理邮件，否则，按照相反的权限进行处理。
附件过滤	选择已经添加的 MAIL 协议关键字，设置邮件附件名称应匹配的关键字。匹配关键字时，将对邮件按照关键字的权限处理邮件，否则，按照相反的权限进行处理。

参数	说明
	说明： 当附件较大使邮件大小超过 1M 限制时，不会对附件名称进行过滤。
邮件正文过滤	选择已经添加的 MAIL 协议关键字，设置邮件正文应匹配的关键字。匹配关键字时，将对邮件按照关键字的权限处理邮件，否则，按照相反的权限进行处理。
登录标题	选择登录标题关键字对象，设置用来替换服务器返回的 Banner 信息的登录标题对象。
转发不符合安全规则的邮件	对于 SMTP 和 POP3 协议，当原邮件命中过滤策略时，可以根据此处的配置，对不符合安全规则的邮件进行转发或不转发处理。 说明： 1) 当设置为“关闭”时，不转发该邮件。 2) 当设置为“打开”时，按 10.1.2警告邮件内容 配置的参数将邮件转发到指定的收件人。如果配置有误，即使打开了此开关，也收不到转发的邮件。

e) 防病毒：

对于 HTTP、FTP、SMTP、POP3 和 IMAP 协议，设置是否启用防病毒模块检查数据包。

▼ 防病毒						
	HTTP	FTP	SMTP	POP3	IMAP	
启用开关	☐	☐	☐	☐	☐	

勾选协议下方的复选框，则启用该协议的防病毒过滤功能。

f) 反垃圾邮件：

设置是否启用反垃圾邮件模块检查 SMTP 协议的数据包，并设置启用哪些方式对垃圾邮件进行拦截。检测的顺序是：白名单、黑名单、反向 DNS、实时黑名单、灰名单。

▼ 反垃圾邮件		
启用邮件黑名单	☐	
启用IP黑名单	☐	
启用邮件白名单	☐	
启用IP白名单	☐	
启用实时黑名单	☐	处理方式 记录
启用反向DNS	☐	处理方式 记录
启用灰名单	☐	

勾选复选框，则启用了相应的反垃圾邮件过滤方式。具体说明如下表：

参数	说明
处理方式	设置邮件地址匹配实时黑名单和反向 DNS 查询时的处理方式。可选项为记录、阻断。
启用邮件黑名单	勾选该选项时，将对邮件发件人的邮件地址进行过滤，检查是否与“邮件地址黑名单”列表中的条目逐个相匹配，如果SMTP协议的源或目的邮件地址命中黑名单，邮件将被拦截并抛弃。如果POP3 协议或IMAP协议的源或目的邮件地址命中黑名单，将在邮件中加入垃圾邮件标记信息。具体参数设置请参见 15.1.1设置邮件地址黑白名单 。
启用 IP 黑名单	勾选该选项时，将对邮件发件人的IP地址进行过滤，检查是否与“IP地址黑名单”列表中的条目逐个相匹配，如果SMTP协议的源或目的IP地址命中黑名单，邮件将被拦截并抛弃。如果POP3 协议或IMAP协议的源或目的IP地址命中黑名单，将在邮件中加入垃圾邮件标记信息。具体参数设置请参见 15.1.2设置IP地址黑白名单 。
启用邮件白名单	勾选该选项时，将对邮件的“发件人”进行过滤，检查是否与“邮件地址白名单”列表中的条目逐个相匹配，命中白名单，将在此处放行邮件。具体参数设置请参见 15.1.1设置邮件地址黑白名单 。
启用 IP 白名单	勾选该选项时，将对邮件发件人的IP地址进行过滤，检查是否与“IP地址白名单”列表中的条目逐个相匹配，如果SMTP协议的源或目的IP命中白名单，邮件将被直接放行。如果POP3 协议或IMAP协议的源或目的IP命中白名单，将在此处放行邮件。具体参数设置请参见 15.1.2设置IP地址黑白名单 。
启用实时黑名单	设置是否开启实时黑名单过滤垃圾邮件。启用该功能后，对于匹配规则的数据报文，网络卫士安全网关将根据实时黑名单（RBL）查询服务来预防垃圾邮件通过安全网关进行传输。具体参数设置请参见 15.2实时黑名单 。
启用反向 DNS	设置是否开启反向域名解析功能进行反垃圾邮件过滤。启动该功能，对于匹配规则的数据报文，将反向查询 IP 地址对应的注册域名，如果发件人 IP 地址没有注册域名，则该 IP 发送的邮件信息将被安全网关标记为垃圾邮件，并根据“处理方式”的设置，拒绝接收邮件或只是记录相关情况。
启用灰名单	设置是否开启灰名单过滤功能。具体参数设置请参见 15.3灰名单技术 。

g) 应用程序识别：

网络卫士安全网关可以对各种类型的应用层的流量进行检测和控制：既支持传统的应用层协议，也支持各种新的应用类型：包括股票交易类应用、即时通讯类应用、流媒体类应用、网络游戏类应用、网络电话类应用、P2P 下载类应用、反动软件类应用、其他流量应用等，而且系统还支持通过自定义应用来扩展新的应用类型。

网络卫士安全网关还支持对流量进行深度检测，以识别出具有P2P软件行为特征的连接。当ACL规则引用该内容安全策略时，对于匹配ACL规则的流量，所有源地址对象中包含的地址都将进行DFI检测。系统将根据在“其他流量”的“疑似P2P”处设置的动作进行处理。设置为“禁止”时，将目的地址加入黑名单，使之在一定时间内不能建立连接；设置为“带宽控制”时，可以通过QoS模块对此连接进行限速。也可以直接将主机加入监控列表中进行P2P行为监控，具体请参见 [11.3主机监控](#)。

▼ 应用程序识别

▶ ☐ 所有协议	允许	▼
▶ ☐ 传统协议	允许	▼
▶ ☐ 股票交易	允许	▼
▶ ☐ 即时通讯	允许	▼
▶ ☐ 流媒体	允许	▼
▶ ☐ 网络游戏	允许	▼
▶ ☐ 网络电话	允许	▼
▶ ☐ 网络电视	允许	▼
▶ ☐ P2P下载	允许	▼
▶ ☐ 其他流量	允许	▼
▶ ☐ 自定义协议	允许	▼

提示: 以下应用要完全阻断或限速，还需要勾选一些其他应用配合

QQ音视频聊天：还需要勾选QQ文件传输

迅雷：还需要勾选伪IE下载、HTTP分块传输、迅雷看看、bt、eDonkey

flashget：还需要勾选伪IE下载、HTTP分块传输、bt、eDonkey

PPLive：还需要勾选web视频

管理员需要设置对于匹配规则的流量，检测和控制哪些应用类型、以及相应的处理动作。

应用类型一共分为 10 个大类（称为“父类”），每一个大类中又分为若干个小的分类（称为“子类”），点击父类协议左侧的蓝色箭头，可以查看到子类协议的详细信息，如下图所示。

▼ 应用程序识别

☐ 所有协议	允许	
☒ 传统协议	允许	
☒ HTTP	带宽控制	QOS: 未选择
☐ HTTP分块传输	允许	
☐ 伪IE下载	允许	
☐ SMTP	允许	
☐ POP3	允许	
☐ SMB	禁止	
☐ TELNET	允许	
☐ SSH	允许	
☐ IMAP	允许	
☐ SSL	允许	
☐ 远程桌面	允许	
☐ DNS	允许	
☐ netbios	允许	
☐ DHCP	允许	
☐ NTP	允许	

管理员可以勾选父类应用，设置对父类中的所有子类的控制策略，如下图所示。

▼ 应用程序识别

☒ 所有协议	允许	
☐ 传统协议	允许	
☐ 股票交易	允许	
☐ 即时通讯	允许	
☐ 流媒体	允许	
☐ 网络游戏	允许	
☐ 网络电话	允许	
☐ 网络电视	允许	
☐ P2P下载	允许	
☐ 其他流量	允许	
☐ 自定义协议	允许	

提示: 以下应用要完全阻断或限速, 还需要勾选一些其他应用配合
 QQ语音视频聊天: 还需要勾选QQ文件传输
 迅雷: 还需要勾选伪IE下载、HTTP分块传输、迅雷看看、bt、eDonkey
 flashget: 还需要勾选伪IE下载、HTTP分块传输、bt、eDonkey
 PPLive: 还需要勾选web视频

也可以分别勾选子类协议，设置对各个子类不同的控制策略。如下图所示。

▼ 应用程序识别			
☐ 所有协议	允许		
☐ 传统协议	允许		
☐ HTTP	允许		
☒ HTTP分块传输	带宽控制		QoS: 未选择
☐ 伪IE下载	允许		

不同的协议所支持的动作操作不同，系统所支持的动作包含如下几类：允许、禁止、带宽控制和账号过滤，释义如下表所示。

动作	说明
允许	允许该类型协议的报文流量通过。
禁止	禁止该类型协议的报文流量通过。
带宽控制	通过引用带宽规则对该类型协议的报文流量进行带宽控制，控制上传及下载的流量，关于带宽规则的设置具体请参见 6.7.1QoS 。 说明： 此处引用的 QoS 对象必须设置为“共享类”，而且不能设置保证带宽。
账号过滤	系统所有未配置到账号过滤中账号（QQ和MSN账号）的默认动作，包括允许和禁止。关于账号过滤的具体配置请参见 11.1账号过滤 。

需要特别说明的是：以下类型的应用要实现完全阻断或限速，必须同时阻断或限速与其相关的其他应用类型。

- QQ 语音视频聊天：还需要设置“QQ 文件传输”策略；
- 飞速土豆和 PP 加速器：还需要设置“web 视频”策略；
- 迅雷和 flashget：还需要设置伪 IE 下载、HTTP 分块传输、bt、eDonkey 策略；
- PPLive：还需要设置“web 视频”策略。

h) 其他协议过滤：

对通过 RSH、TELNET 传输的命令进行关键字过滤，对通过设备的 DNS 查询请求进行域名过滤。如下图，勾选相应协议后才对匹配 ACL 规则的相应协议的数据启用过滤功能。

▼ 其他协议过滤			
	TELNET	RSH	DNS
命令控制	未选择	未选择	未选择
登录标题替换	未选择		

参数说明如下表所示：

参数	说明
命令控制	设置进行内容过滤的命令具备的特征。当通过设备的相应协议的命令匹配选中的关键字对象时，根据关键字对象的权限对命令进行处理。
登录标题替换	指用来替换服务器返回的 Banner 信息的登录标题对象。

i) 记录日志：

设置当匹配规则的情况发生时，是否在日志中记录相关信息。默认情况下，网络卫士安全网关不记录深度内容过滤相关的日志信息。

▼ 记录日志	
协议	日志
HTTP过滤	☐
FTP过滤	☐
WEB过滤	☐
邮件过滤 (SMTP)	☐
邮件过滤 (POP3)	☐
邮件过滤 (IMAP)	☐
反垃圾邮件	☐
应用程序识别	☐
其他协议过滤 (TELNET)	☐
其他协议过滤 (RSH)	☐
其他协议过滤 (DNS)	☐

设置完参数后，点击“确认”完成对象设置。

10 内容过滤

通过配置内容过滤策略，并且在访问控制规则中引用该策略，网络卫士安全网关可以实现对应用层的流量的检测和控制。系统通过深入读取 IP 包载荷的内容来对 OSI 七层协议中的应用层信息进行重组，从而得到整个应用程序的内容，然后按照系统定义的管理策略对流量进行整形操作。网络卫士安全网关不仅支持对传统的应用层协议进行配置及深度内容检测，而且支持各种新的应用类型，系统还支持通过自定义应用来扩展新的应用类型。

本章内容主要包括：

- 邮件过滤：介绍如何设置邮件过滤的关键字对象，以及如何设置警告邮件内容。
- HTTP 过滤：介绍 HTTP 过滤的 URL 关键字，以及网页内容和 HTTP 过滤的关键字对象。
- 其他协议过滤：主要介绍如何设置其他协议的关键字和登录标题对象。
- 应用端口绑定：介绍如何设置协议与非常用端口的绑定策略。

说明

✧ 本章中配置的内容过滤策略只有在防火墙的访问控制规则中引用，才能够生效。

10.1 邮件过滤

网络卫士安全网关根据 ACL 策略中引用的内容安全策略，对通过设备的数据包的内容进行检测。如果在所引用的内容安全策略中开启了邮件过滤功能，网络卫士安全网关将对通过设备的邮件进行检查，当邮件匹配 SMTP DPI 策略、POP3 DPI 策略时，根据策略设置的关键字权限（允许或拒绝）进行处理；否则系统将按照与关键字权限相反的权限对数据进行处理。对于邮件，则可能丢弃该邮件的全部或其附件，也可能将原邮件转发到指定人员。本节内容包括：

- （1）配置邮件过滤关键字
- （2）配置警告邮件内容

10.1.1 内容过滤

关键字对象是定义内容安全策略的基础。管理员需要定义邮件的关键字对象，并在内容安全策略中开启邮件过滤功能和引用关键字对象，安全网关才能对通过设备的邮件内容

进行过滤。当数据匹配关键字时，按照关键字的权限（允许或拒绝）进行处理；否则系统将按照与关键字权限相反的权限对数据进行处理。

增加邮件过滤关键字对象的具体步骤如下所示：

1) 在左侧导航菜单中选择 **内容过滤** > **邮件过滤**，并激活“内容过滤”页签，界面如下图所示。

2) 添加对象

a) 点击“添加”，进入“关键字属性”界面，如下图所示。

关键字属性的参数说明如下表所示。

参数	说明
名称	指关键字对象的名称。
关键字	指要过滤的敏感内容。可以通过点击“区分大小写”前面的复选框，确定是否在过滤时对关键字的大小写进行区分。 说明： 参数值是支持通配符 *（表示多个字符）和 ?（表示任意一个字符）的字符串，最多不能超过 255 个字符。
类型	设置匹配该关键字时的访问权限。可选项为“允许”和“禁止”，分别表示该协议传输的内容中包含该关键字时，系统的操作权限为允许或禁止。否则系统将按照与关键字权限相反的权限对数据进行处理。

b) 参数值设置完成后，点击“确定”按钮，完成添加；点击“取消”按钮，取消此次操作。

3) 修改对象属性

在“关键字”界面中，点击“修改”一列对应的图标，可以修改该关键字的属性。

4) 删除对象

点击“删除”一列对应的图标，如果该关键字未被引用，可以删除该关键字对象；点击“清空”，可以清空所有未被引用的关键字对象。

10.1.2 警告邮件内容

当邮件匹配 SMTP DPI 策略、POP3 DPI 策略时，根据策略设置，可能丢弃该邮件的全部或其附件，也可能将原邮件转发到指定人员。

当邮件处理方式设置为“丢弃”时，安全网关系统会向指定人员发送告警邮件，告警邮件的主题和内容可以使用系统默认设置，管理员也可以进行更改；当邮件处理方式设置为转发时，还需指定邮件的收件人，另外还需设置发件人的地址信息，邮件帐户名和密码信息，以及该帐户的SMTP服务器地址，具体请参见 [4.2.5邮件设置](#)。

设置邮件过滤相关参数的具体步骤为：

1) 在左侧导航菜单中选择 **内容过滤** > **邮件过滤**，并激活“警告邮件”页签，界面如下图所示。

The screenshot shows a configuration window titled "警告邮件" (Warning Email) with a sub-tab "警告邮件内容" (Warning Email Content). The window contains the following fields and controls:

- 邮件主题 (Email Subject):** A text input field with the default value "此邮件违反了安全策略" (This email violates security policy).
- 邮件正文 (Email Body):** A text area with a scroll bar. It contains the text: "网关提示: ***** 此邮件违反了安全策略, 被过滤 *****".
- 转发不符合安全规则的邮件 (Forward emails that do not conform to security rules):** A section header for the forwarding configuration.
- 收件人地址 (Recipient Address):** A text input field.
- 确定 (OK):** A button at the bottom center of the window.

参数说明如下表所示：

参数	说明
邮件主题	设置安全网关系统发送的提示邮件的邮件主题。 说明： 当存在被 POP3 邮件过滤策略或 IMAP 邮件过滤策略拦截的邮件时，安全网关系统才会向原收件人发送该提示邮件。
邮件正文	设置安全网关系统发送的提示邮件的内容。 说明： 当存在被 POP3 邮件过滤策略或 IMAP 邮件过滤策略拦截的邮件时，安全网关系统才会向原收件人发送该提示邮件。
收件人地址	设置接收非法邮件（即不符合安全规则的邮件）的电子邮箱地址。 说明： 1) 只有 防火墙 > 内容安全策略 > 邮件过滤 处的“转发不符合安全规则的邮件”打开后，该项设置才能有效。 2) 只能转发通过 SMTP 发送或通过 POP3 接收的邮件。

2) 点击“确定”按钮，系统保存参数设置。

10.2 HTTP 过滤

HTTP 过滤用于设置 HTTP 协议过滤所需的关键字对象。本节内容包括：

- (1) URL 过滤：用于设置 URL 关键字对象。
- (2) 内容过滤：用于设置网页内容过滤关键字和 HTTP 头过滤的关键字对象。

10.2.1 URL 过滤

URL 对象是 HTTP 过滤 URL 的基础，可以根据需要过滤对敏感 URL 的访问。设置 URL 对象的具体步骤如下所示：

1) 在左侧导航菜单中选择 **内容过滤 > HTTP过滤**，并激活“URL过滤”页签，界面如下图所示。

URL过滤			
内容过滤			
+ 添加 🗑️ 清空 总计: 0			
名称	URL	类型	操作

2) 添加对象

a) 点击“添加”，进入“URL 属性”界面，如下图所示。



URL属性

名称 *

URL

<-

×

类型 ☐ 允许 ☒ 禁止
(例如: *sina可以匹配所有包含sina的URL, 如 news.sina.com.cn等)

确定 取消

URL 属性的参数说明如下表所示。

参数	说明
名称	指 URL 对象的名称。
URL	指要过滤的敏感 URL 地址。 说明: 1. 参数值是字符串 (包括 IP 地址和域名), 不支持正则表达式, 但支持通配符 “*”。 2. 最多不能超过 255 个字符。 3. 一个汉字占用两个字符。
类型	指匹配该 URL 的访问权限。 说明: 选中 “允许” 表示允许访问该 URL; 选中 “禁止” 表示禁止访问该 URL。

b) 参数值设置完成后, 点击 “确定” 按钮, 完成添加; 点击 “取消” 按钮, 取消此操作。

3) 修改对象属性

在 “URL” 界面中, 点击 “修改” 一列的对应图标, 可以修改该 URL 的属性。

4) 删除对象

点击 “删除” 一列的对应图标, 可以删除该 URL 对象; 点击 “清空”, 可以清空所有未被引用的 URL 对象。

10.2.2 内容过滤

关键字对象是定义内容安全策略对象的基础。管理员通过定义 HTTP 过滤的关键字对象, 并在内容安全策略中开启 HTTP 过滤功能, 并引用 HTTP 协议的关键字对象, 安全网

关对通过设备传输的 HTTP 协议的内容进行过滤。当数据匹配关键字时，按照关键字的权限（允许或拒绝）进行处理；否则系统将按照与关键字权限相反的权限对数据进行处理。

增加关键字对象的具体步骤如下所示：

1) 在左侧导航菜单中选择 **内容过滤** > **HTTP过滤**，并激活“内容过滤”页签，界面如下图所示。

名称	关键字	区分大小写	类型	操作
总计: 0				

2) 添加关键字

a) 点击“添加”，界面如下图所示。

关键字属性的参数说明如下表所示。

参数	说明
名称	指关键字对象的名称。
关键字	设置要过滤的敏感内容。可以通过点击“区分大小写”前面的复选框，确定是否在过滤时对关键字的大小写进行区分。 说明： 参数值是支持通配符 *（表示多个字符）和 ?（表示任意一个字符）的字符串，最多不能超过 255 个字符。而且，通配符 * 和 ? 只可以出现关键字中间，关键字首尾不可以配置通配符 * 和 ?。否则系统会提示错误信息。
类型	不需要设置该选项。HTTP 协议传输的内容中包含该关键字时，系统的操作权限为禁止。

b) 参数值设置完成后，点击“确定”按钮，完成添加；点击“取消”按钮，取消此次操作。

3) 修改对象属性

在“关键字”界面中，点击“修改”一列对应的图标，可以修改该关键字的属性。

4) 删除对象

点击“删除”一列对应的图标，如果该关键字未被引用，可以删除该关键字对象；点击“清空”，可以清空所有未被引用的关键字对象。

10.3 其他协议过滤

本节介绍如何设置 FTP、TELNET、DNS 和 RSH 协议过滤策略中引用的关键字对象，以及登录标题对象。

10.3.1 关键字对象

关键字对象是定义内容安全策略对象的基础，根据协议的不同，管理员可以定义 FTP 过滤、RSH 过滤、TELNET 过滤和 DNS 过滤的关键字对象，并在内容安全策略中引用该关键字对象，则当通过安全网关传输的数据匹配关键字时，按照关键字的权限（允许或拒绝）进行处理；否则系统将按照与关键字权限相反的权限对数据进行处理。

增加关键字对象的具体步骤如下所示：

1) 在左侧导航菜单中选择 **内容过滤** > **其他协议过滤**，并激活“关键字”页签，界面如下图所示。

关键字		登录标题			
+ 添加		清空		总计: 0	
名称	关键字	区分大小写	协议	类型	操作

2) 添加对象

a) 点击“添加”，进入“关键字属性”界面，如下图所示。

关键字属性

名称 *

关键字

<

X

☐ 区分大小写

协议 FTP ▼

类型 ☐ 上传 ☐ 下载

确定
取消

关键字属性的参数说明如下表所示。

参数	说明
名称	指关键字对象的名称。
关键字	指要过滤的敏感内容。可以通过点击“区分大小写”前面的复选框，确定是否在过滤时对关键字的大小写进行区分。 说明： 参数值是支持通配符 *（表示多个字符）和 ?（表示任意一个字符）的字符串，最多不能超过 255 个字符。
协议	指该关键字匹配的协议类型。 可选值为：FTP、RSH、TELNET 和 DNS。
类型	设置匹配该关键字时的访问权限。选择不同的协议类型时显示不同的选项。 说明： 1. 当“协议”选择“FTP”时可选项为上传和下载，选择“上传”表示当文件名匹配该关键字时允许上传，选择“下载”表示当文件名匹配该关键字时允许下载。不选择时表示表示当文件名匹配该关键字时禁止上传和下载。 2. 当“协议”选择“TELNET”时不需要设置该选项。 3. 当“协议”选择“RSH”和“DNS”时，可选项为“允许”和“禁止”，分别表示该协议传输的内容中包含该关键字时，系统的操作权限为允许或禁止。

b) 参数值设置完成后，点击“确定”按钮，完成添加；点击“取消”按钮，取消此次操作。

3) 修改对象属性

在“关键字”界面中，点击“修改”一列对应的图标，可以修改该关键字的属性。

4) 删除对象

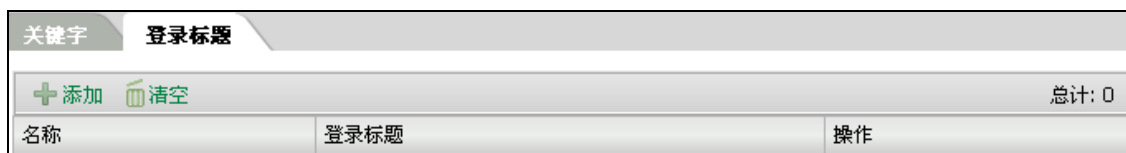
点击“删除”一列对应的图标，如果该关键字未被引用，可以删除该关键字对象；点击“清空”，可以清空所有未被引用的关键字对象。

10.3.2 登录标题对象

服务器向客户端返回的 Banner 信息中往往提供了服务器的版本号等敏感信息，网络卫士安全网关支持在内容过滤策略中使用登录标题对象来替换这些信息，从而保护服务器的版本信息不被暴露。

配置登录标题对象的具体步骤介绍如下：

1) 在左侧导航菜单中选择 **内容过滤** > **其他协议过滤**，并激活“登录标题”页签，界面如下图所示。



2) 添加对象

a) 点击“添加”，进入“登录标题属性”界面，如下图所示。

登录标题属性的参数说明如下表所示。

参数	说明
名称	指登录标题对象的名称。
登录标题	指用来替换服务器返回的 Banner 信息的字符串，最多不能超过 255 个字符。

b) 参数值设置完成后，点击“确定”按钮，完成添加；点击“取消”按钮，取消此操作。

3) 修改对象属性

点击指定对象后面“修改”一列对应的图标，可以修改该对象的属性。

4) 删除对象

点击指定对象后面“删除”一列对应的图标，可以删除该对象；点击“清空”，可以清空所有未被引用的登录标题对象。

10.4 应用端口绑定

一般情况下，常用的应用层协议采用众所周知的端口号为用户提供服务。如果个别用户网络中采用非标准端口向用户提供服务，则必须添加新的端口绑定策略，否则，不能根据已有的访问控制规则对应用层的数据进行深度内容检测，容易对内部网络造成安全隐患。

对于多连接协议，除了建立一个主连接外，还会动态建立一些子连接进行通信。管理员添加应用协议和相应的传输协议及端口的绑定策略后，新建连接时安全网关会动态地开放子连接的端口，并在连接结束时自动关闭。能够在保证安全网关和网络安全的情况下，允许多连接协议的流量通过安全网关。

应用端口绑定的具体操作步骤如下所示：

1) 在左侧导航菜单中选择 **内容过滤** > **应用端口绑定**，界面如下图所示。

应用端口绑定			
+ 添加 重置 清空			总计: 5
应用协议类型	协议/端口	目的子网/掩码	操作
ftp	tcp/21	0.0.0.0/0.0.0.0	  
smtp	tcp/25	0.0.0.0/0.0.0.0	  
tftp	udp/69	0.0.0.0/0.0.0.0	  
http	tcp/80	0.0.0.0/0.0.0.0	  
pop3	tcp/110	0.0.0.0/0.0.0.0	  

系统默认定义了部分应用层协议与标准端口的绑定，包括 FTP、SMTP、TFTP、HTTP、POP3、SQLNET 和 TELNET 协议。

点击“操作”栏的图标“”或“”可以启用或禁用该策略，禁用后该规则将无效。

2) 添加端口绑定策略

a) 点击“添加”，进入“应用协议端口绑定”界面，如下图所示。

“应用协议端口绑定”界面的参数说明如下表所示。

参数	说明
应用协议	指需要进行绑定的应用层协议类型。 包括：HTTP、FTP、TFTP、SMTP、POP3、IMAP、TELNET、MMS、H225、H225RAS、RSH、SIP、RTSP、PPTP、DNS、SUN_RPC、MS_RPC、NETLOGIN 和 SQLNET。 说明： H.323 标准协议簇，它包含多种通信协议，因此在应用端口绑定中没有 H.323 协议选项。要保证 H.323 协议通过安全网关正常的流量传输，需要在绑定 H.225 与 TCP 端口 1720 的同时，将 H.225RAS 与 UDP 的 1719 端口进行绑定。
协议类型	指相应的传输层协议类型。 包括：TCP 和 UDP。
端口	指应用层协议使用的端口号。
目的子网	输入子网地址或主机 IP 地址字符串，表示对去往某些特定子网或特定主机的报文建立自定义端口号和应用协议的识别。例如：将去往 10.110.0.0 网段的主机使用 8080 端口的 TCP 报文识别为 HTTP 报文。 说明： 设置为 0.0.0.0，表示所有子网都适用该绑定策略。
子网掩码	指目的子网掩码。 当“目的子网”设定为主机 IP 地址时，此处应当输入 255.255.255.255。
启用规则	指是否启用该绑定规则，默认启用该规则，不选表示该规则暂不生效。 说明： 点击“操作”栏的图标“”或“”可以启用或禁用该策略，禁用后该规则将无效。

b) 参数值设置完成后，点击“确定”按钮，完成添加；点击“取消”按钮，取消此次操作。

3) 对于已有规则，点击“修改”一列对应的图标可以修改该规则。

4) 删除规则

点击“删除”一列对应的图标，可以删除该规则；点击“清空”，可以清空所有的规则。

5) 点击“重置”，可以将端口绑定策略恢复为系统的出厂配置。

说明

-
- ✧ 由于 SIP 协议可能通过 TCP 和 UDP 方式传输，所以需根据实际应用分别设置 TCP 和 UDP 与应用端口的绑定策略，默认情况下 SIP 使用 UDP 的 5060 端口进行通信。
-

11 应用识别

网络卫士安全网关全面支持对即时通讯软件（如：MSN、QQ、网易泡泡、新浪 UC、Yahoo! Messenger、阿里旺旺、迅雷和 SKYPE）以及 P2P 协议（如：BT, eMule 和 eDonkey）的应用和访问控制。

本章内容主要包括：

- 账号过滤：介绍如何配置 MSN 和 QQ 的账号对象，并查看在线的 MSN 用户信息。
- 自定义应用：介绍如何自定义应用识别规则；
- 主机监控：主要介绍如何监控和查看主机的 P2P 行为；
- P2P 行为识别：主要介绍如何开启设备的 P2P 行为识别功能；
- 流量异常检测：主要介绍如何设置异常流量的阈值。

11.1 账号过滤

网络卫士安全网关提供对 MSN、QQ 等即时聊天软件的帐号进行过滤的功能，能指定特别的 MSN、QQ 帐号允许，禁止其他帐号；也可以指定特别的 MSN、QQ 帐号禁止，允许其他帐号。

管理员需要首先添加帐号信息，然后再策略中引用帐号，从而实现对帐号的控制。

帐号对象是应用程序识别帐号过滤的基础，可以根据帐号限制或允许某些帐号登录。设置帐号对象的具体步骤如下所示：

- 1) 在左侧导航菜单中选择 **应用识别 > 账号过滤**，界面如下图所示。

帐号						
+ 添加		清空		总计: 0		
名称	帐号	帐号类别	类型	状态	修改	删除

- 2) 添加新的账号对象。

- a) 点击“添加”，进入“账号属性”界面，如下图所示。

帐号属性的参数说明如下表所示。

参数	说明
名称	输入帐号对象的名称。
帐号类型	选择帐号类型，可选项为 QQ、MSN。
帐号	设置指要过滤的帐号，以空格隔开。 说明： 1. 帐号类型是 QQ 时，帐号应为数字，帐号类型为 MSN 时，帐号应为合法的 Email 地址。 2. 帐号总长不超过 1024 字节
类型	设置禁止还是允许该帐号通过安全网关。
是否启用	设置是否启用该帐号，只有启用后该帐号才生效。

b) 参数值设置完成后，点击“确定”按钮，完成添加；点击“取消”按钮，取消此次操作。

3) 修改帐号属性

在“帐号”界面中，点击指定帐号后面“修改”一列对应的图标“”，可以修改该帐号的属性。

4) 删除帐号对象

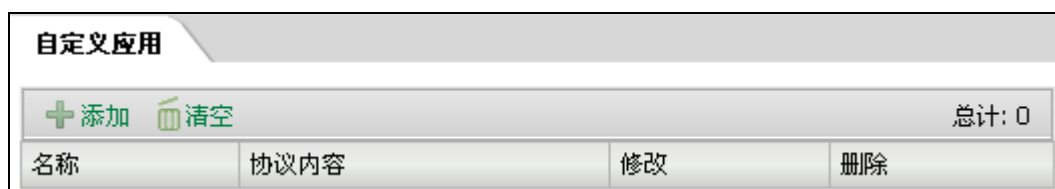
点击指定帐号后面“删除”一列对应的图标“”，可以删除该帐号对象；点击“清空”，可以清空所有未被引用的帐号对象。

11.2 自定义应用

除了系统自带的应用识别规则库，网络卫士安全网关系统也允许用户根据特定的需要自行定义应用协议。设置好的自定义应用协议会自动添加到系统规则库，供用户在“内容安全策略”中设置应用识别规则时引用，具体请参见[应用识别规则](#)。

具体操作步骤如下：

- 1) 在左侧导航菜单中选择 **应用识别** > **自定义应用**，界面如下图所示。



- 2) 点击“添加”，界面如下图所示。

参数说明如下表所示：

参数	意义
名称	输入自定义应用的对象名称。
协议类型	选择自定义应用使用的协议类型。可选值为：TCP、UDP。
端口号	输入自定义应用占用的端口号。

点击“确定”，完成设置。点击“取消”放弃添加。

11.3 主机监控

网络卫士安全网关支持对被监控主机的流量进行深度检测，以识别出具有P2P软件行为特征的连接，并对受攻击主机排名和应用主机排名，关于排名的具体信息请参见[5.4.2受攻击主机排名](#)和[5.6.2应用主机排名](#)。对主机进行流量监控有两种设置方法：

(1) 管理员通过在内容安全策略中定义“应用程序识别”规则，在“其他流量”的“疑似 P2P”处设置对疑似 P2P 协议的处理权限。当 ACL 规则引用该内容安全策略时，对于匹配 ACL 规则的流量，所有源地址对象中包含的地址都将进行 DFI 检测。

(2) 直接将主机加入监控列表中进行 P2P 行为监控。具体操作步骤如下：

1) 选择 **应用识别 > 主机监控**，如下图所示。

主机监控		
+ 添加 清空		
名称	监控范围	操作
server1	server1	  
dd	server2	  
mo2	host1	  

2) 点击“添加”，设置需要监控的主机，如下图。

主机监控

名称 *

备选

server1 [主机]
host1 [主机]
server2 [主机]
any [范围]

->
×

已选

确定

取消

3) 设置监控名称，并在在备选地址资源里选中要监控的资源对象，然后点击“→”将其添加到已选栏内，监控主机可以添加多个；在已选栏内选用地址，点击“×”可将删除。

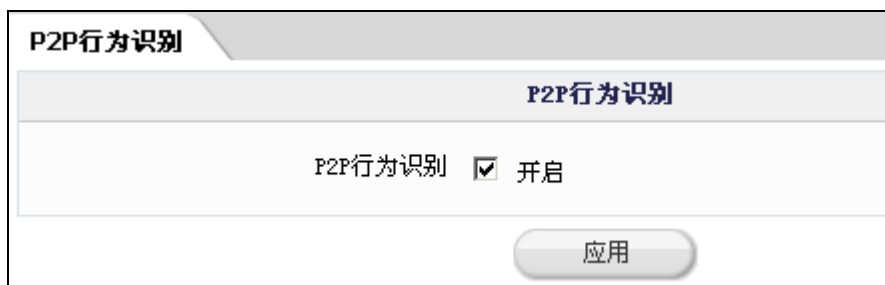
4) 监控主机选择完毕后，点击“确定”即可。

5) 点击操作栏中的“ ”或“ ”图标，可以对主机监控策略进行禁用和启用操作，被禁用的主机监控策略背景为灰色。

11.4 P2P 行为识别

只有开启了 P2P 行为识别功能，才能对“主机监控”中设置的主机进行 P2P 行为识别的监控。

- 1) 选择 **应用识别 > P2P行为识别**，如下图所示。



- 2) 通过勾选或反选“开启”项，可以开启或关闭 P2P 行为识别功能。
- 3) 点击“应用”按钮，使设置生效。

11.5 流量异常检测

网络卫士安全网关支持基于物理接口、协议等流量异常检测功能，在统计的基础上对接口流量和监控应用协议组的相关指标设定阈值并制定相应的报警规则，当统计值大于设定值时进行报警。关于报警规则的设置请参见[17.3.1添加报警规则](#)。

管理员可对以下几种类型的参数设置阈值：

- 对应用协议组流量以及应用协议组连接数设置阈值，超出阈值则报警，报警间隔 1 分钟。触发报警规则后，在 **系统监视 > 应用统计** 界面也会亮起相应的报警灯（红色表示有报警）。
- 对每个物理接口的流量值设置阈值，超出阈值则报警，报警间隔为 1 分钟。触发报警规则后，在 **系统监视 > 接口流量** 的各接口的界面也会亮起相应的报警灯（红色表示有报警）。
- 对协议比例（TCP 流量占总流量、UDP 流量占总流量、其他流量占总流量）设置阈值，超出阈值则报警，报警间隔 1 分钟。
- 对最大连接数设置阈值，超出阈值则报警，报警间隔 1 分钟。

具体操作如下：

选择 **流量管理 > 流量异常检测**，如下图所示。

协议组阈值				
	流量阈值 (单位: KByte/s)		连接数 (单位: 个)	
传统协议	0	[0-512000]	0	[0-1000000]
股票交易	0	[0-512000]	0	[0-1000000]
即时通讯	0	[0-512000]	0	[0-1000000]
流媒体	0	[0-512000]	0	[0-1000000]
网络游戏	0	[0-512000]	0	[0-1000000]
网络电话	0	[0-512000]	0	[0-1000000]
网络电视	0	[0-512000]	0	[0-1000000]
P2P下载	0	[0-512000]	0	[0-1000000]
其他流量	0	[0-512000]	0	[0-1000000]
自定义协议	0	[0-512000]	0	[0-1000000]

接口阈值	
	流量阈值 (单位: MByte/s)
接口 eth0	0 [0-250]
接口 eth1	0 [0-250]
接口 eth2	0 [0-250]
接口 eth3	0 [0-250]

协议比例异常阈值	
	比例阈值 (单位: %)
Tcp流量占总流量	0 [0-100]
Udp流量占总流量	0 [0-100]
其他流量占总流量	0 [0-100]

最大连接数阈值	
最大连接数阈值	0 [0-1000000个]

点击“开启”启动流量异常检测模块，点击“停止”停止流量异常检测；各项阈值设置完成后，点击“设置”启用新设参数。

说明

- ◇ 启动流量异常检测功能后，如果将阈值设置为 0 则表示仅对该参数进行检测，不进行报警。

12 PKI 设置

网络卫士安全网关支持对远程用户和隧道对端设备进行数字证书认证。安全网关内置 CA 中心, 可以为设备及用户签发证书并对证书进行管理。安全网关还支持采用第三方 CA 签发的证书对用户和设备进行认证。对于第三方 CA 签发证书, 支持证书状态的离线验证和在线验证。离线认证是指利用颁发者证书和证书撤销列表 (CRL) 来验证签名证书的有效性, 需要在设备上导入 CA 证书和 CRL 列表。在线认证是指通过向轻目录访问协议 (LDAP) 服务器和在线证书状态协议 (OCSP) 服务器在线查询证书是否有效。

本章主要内容包括:

- **本机证书:** 主要介绍如何为安全网关设置设备证书, 该证书主要用于在建立 VPN 隧道时进行身份认证。
- **第三方 CA 证书:** 介绍如何在安全网关上导入第三方 CA 证书和 CRL 列表。
- **本地 CA 策略:** 介绍安全网关内置的 CA 中心如何设置 CA 根证书, 如何对设备或移动用户进行数字证书的发放、查看、导出、写入 USBKey、撤销、删除等操作, 以及如何对 CRL 列表进行维护。
- **USBKEY:** 介绍如何开启安全网关上的 USBKey 接口。
- **远程证书认证:** 介绍如何开启第三方 CA 的证书在线认证功能并设置服务器的相关信息。
- **证书请求:** 介绍如何生成证书请求, 以及如何导入第三方 CA 服务器根据证书请求文件签发的证书文件。
- **备份和恢复:** 介绍如何对安全网关中保存的证书文件进行维护, 包括证书文件的恢复和下载功能。

12.1 本机证书

本机证书是指由安全设备与策略管理系统 TopPolicy (以下简称 TP) 或 CA 机构下发的本设备的证书。设备之间可以根据对方的证书信息验证对方身份的合法性。

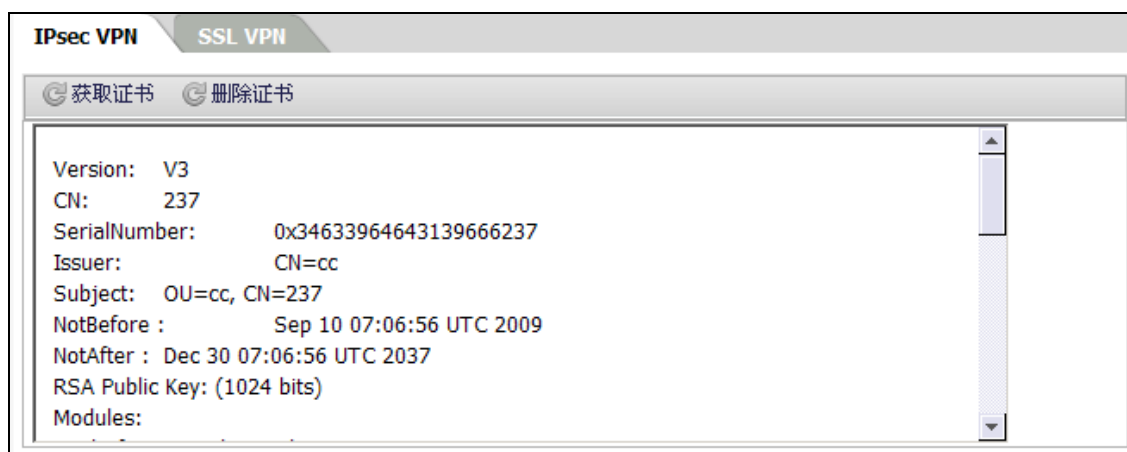
TopPolicy (以下简称 TP) 是由天融信开发的安全设备与策略管理系统, 由其下发的证书包括 3 个部分: 根证书、设备证书和私钥, 分别以 3 个独立的存盘文件存在, 可以存储在硬盘或 USBKEY 等存储载体中。根证书是证书发行机构的自身证书, 可以用来验证该发行机构所发行的证书的合法性。设备证书中包含证书持有者的身份信息、公钥及 CA 发行机构的数字签名, 在网络通讯中标识证书持有者的身份。私钥文件是存放私钥的文件, 与证书中的公钥组成一对互相匹配的公私钥对, 是基于证书的加密体系的重要部分。私钥

文件是证书持有人的私有文件，需要妥善保管。私钥文件有私钥保护密码保护，在一定程度上避免私钥丢失被其他人利用。

由于出厂配置中安全网关没有本机证书，因此需要管理员手工导入。本机证书的导入需要将上述的设备证书和私钥从存储载体中导入到安全网关中。

12.1.1 配置 IPsec VPN 网关证书

1) 点击导航菜单 **PKI设置 > 本机证书**，然后激活“IPsec VPN”页签，如果用户已导入了本机证书，界面如下图所示。



图中文本框显示的证书信息主要包括“证书名称”、“颁发者”、“生效日期”、“失效日期”等。出厂配置中证书为空，需要管理员导入证书。

2) 获取证书。

a) 点击页面右上方的“获取证书”，可以为安全网关设备导入 IPsec VPN 网关证书，如下图所示。

IPsec VPN 网关证书导入

☒ 证书私钥文件

 证书文件

 私钥文件

☐ PKCS12文件

 证书文件

 证书文件密码

☐ TAR文件

 TAR证书文件

☐ USB导入

 PIN码

IPsec VPN 网关证书有四种不同的导入方式：

- 文件方式导入：点击“浏览...”按钮，然后在“选择文件”窗口中选择管理主机上存放的证书文件和私钥文件。
- PKCS12 文件格式导入：首先点击“浏览...”按钮，在“选择文件”窗口中选择管理主机上存放的 PKCS12 标准密钥文件的证书；然后在“证书文件密码”处输入导出证书文件时设置的密码。
- TAR 文件方式导入：点击“浏览...”按钮，然后在“选择文件”窗口中选择管理主机上存放的 TAR 文件（TAR 文件包括打包后的证书、私钥和根证书）。由于不必像第一种方式那样一一指定各个文件的存放路径，所以比较方便。
- USB 导入：首先将存储了证书的 USBKEY 插入到管理主机的 USB 接口，然后正确输入该 USBKEY 的 PIN 码。

b) 在选择好证书导入方式和正确输入相关的选项信息后，点击“确定”按钮，导入证书。证书导入成功后，将会在“本机证书”中显示新导入的证书信息。

说明

- ✧ 每台设备只能有一份证书以验证其身份。如果管理员导入第二份证书，将自动覆盖以前所导入的证书。
- ✧ TAR 方式导入本机证书的同时也导入了 CA 证书，因此无须单独导入 CA 证书。

3) 删除证书。

a) 点击页面右上方的“删除证书”，弹出确认窗口，如下图所示。



b) 点击“确定”按钮，即可删除该证书。

12.1.2 配置 SSL VPN 网关证书

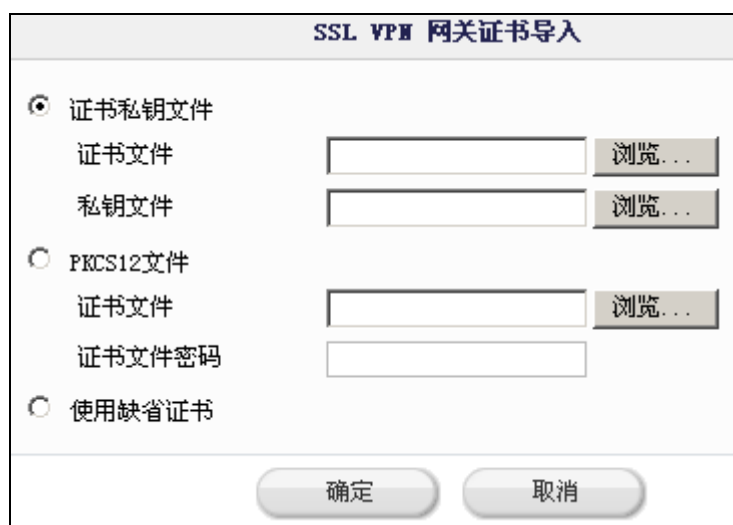
1) 点击左侧导航菜单 **PKI设置 > 本机证书**，然后激活“SSL VPN”页签，下方将显示SSL VPN网关的证书，如下图所示。



在出厂配置中内置了本机证书，图中文本框用来显示证书信息，主要包括了“证书名称”、“颁发者”、“生效日期”、“失效日期”等。

2) 导入 SSL VPN 网关证书

a) 点击页面右上方的“获取证书”，可以导入 SSL VPN 网关证书，界面如下图所示。



SSL VPN 网关证书有三种不同的导入方式：

- 文件方式导入：点击“浏览...”按钮，然后在“选择文件”窗口中选择管理主机上存放的证书文件和私钥文件。
- PKCS12 文件格式导入：首先点击“浏览...”按钮，在“选择文件”窗口中选择管理主机上存放的 PKCS12 标准密钥文件的证书；然后在“证书文件密码”处输入导出证书文件时设置的密码。
- 使用缺省证书：这种方式下将出厂的默认配置证书作为本机证书。

b) 在选择好证书导入方式和正确输入相关的选项信息后，点击“提交设定”按钮，导入证书。证书导入成功后，将会在“本机证书”中显示正确的证书信息。

说明

- ◇ 每台设备只能有一份 SSL VPN 证书以验证其身份。如果管理员导入第二份证书，将自动覆盖以前所导入的证书。

3) 导入证书链

证书链建立一条从证书颁发机构 (CA) 到单个证书的“信任链”。如果可以在根证书目录中找到来自该 CA 的有效证书，就建立了信任。只要您信任 CA，您将自动信任该 CA 签署的任何其他证书。

点击“证书链导入”，界面如下图所示。

该截图显示了一个名为“证书链导入”的对话框。对话框顶部有一个标题栏，下方是一个文本输入框，左侧标有“证书链文件”，右侧有一个“浏览...”按钮。在“浏览...”按钮右侧，有一行红色的提示文字：“[请选择*.p7b格式文件]”。对话框底部有两个按钮，分别是“确定”和“返回”。

点击“浏览”，选择 P7B 格式的证书链文件，然后点击“确定”按钮即可。

12.2 第三方 CA 证书

安全网关支持采用第三方CA颁发的证书对隧道对端设备或移动用户进行认证。当安全网关之间建立采用证书认证的隧道时，需要在此导入对端证书的颁发机构CA的根证书。另外，当VRC客户端采用CA颁发的证书登录安全网关，安全网关在本地认证该用户时，亦需要在此导入该CA的根证书。在这种方式下，安全网关将通过第三方CA的根证书验证客户端证书是否合法。导入CA证书后，可以设置该CA的CRL自动下载协议、下载地址等，也可以手工导入CRL。CA证书管理包括CA证书和CRL的导入、刷新、删除，CRL自动下载管理等操作。安全网关支持同时导入**多个**CA根证书。

说明

- ✧ 如果证书不是根 CA 签发的，则在此需要导入上一级 CA 证书直到根 CA 的证书。

12.2.1 配置 CA 根证书

管理员可以对第三方 CA 证书进行设置，包括 CA 证书的导入、查看和删除，以及 CRL 文件的手动导入，查看和删除。

- 1) 选择左侧导航菜单 **PKI设置** > **第三方CA证书**，如下图所示。

第三方CA证书									
导入CA		配置CRL自动下载							总计: 1
证书名称	有效期	详细信息	CA删除	CRL	CRL属性	CRL导入	CRL下载设置	CRL下载	CRL删除
cc	Aug 20 08:04:40 UTC 2009- Dec 31 08:04:40 UTC 2037			no					

- 2) 点击页面右上方的“导入 CA”，导入第三方 CA 证书，界面如下图所示。

导入CA证书

CA证书文件

浏览...

证书撤销列表文件

浏览...

确定

取消

输入 CA 证书和证书撤销列表文件（CRL）的存放路径，或者点击“浏览...”按钮选择管理主机上存放的 CA 证书文件和证书撤销列表文件。

参数设定完成后，点击“确定”按钮，导入证书。证书导入成功后，将会在“CA 证书维护”页面中显示正确的证书信息。

- 3) 点击新增第三方 CA 证书的“详细信息”图标，可以查看该证书的详细内容。

- 4) 点击待删除第三方 CA 证书的“CA 删除”图标，可以删除该证书。

5) 如需手动更新 CRL 列表，可点击待下载 CRL 的第三方 CA 证书条目右侧的“CRL 导入”图标，如下图所示。

导入CRL

crl文件

浏览...

确定

取消

输入 CRL 文件的路径，或者点击“浏览...”按钮在管理主机上选择该 CRL 文件。

参数设定完成后，点击“确定”按钮即可。

6) 当第三方 CA 证书条目右侧的“CRL”图标显示为“yes”时，可以通过点击“CRL 属性”图标查看该 CA 证书的 CRL 文件信息。

7) 点击待删除 CRL 的第三方 CA 证书条目右侧的“CRL 删除”图标，可以删除该 CA 证书的 CRL 列表信息。删除后证书对应的“CRL”一列显示为“no”，“CRL 删除”一列显示为“-”。

12.2.2 配置 CRL 自动下载

安全网关支持第三方 CA 证书的 CRL 手工更新，也支持 CRL 自动下载，设置自动下载后安全网关将会定时自动下载更新 CRL 文件。

配置第三方 CA 证书的 CRL 自动下载的具体步骤如下所示：

1) 选择左侧导航菜单 **PKI设置 > 第三方CA证书**。

2) 设置下载服务器信息。

点击待下载 CRL 的第三方 CA 证书条目右侧的“CRL 下载设置”图标。

如果选择通过 LDAP 方式下载，界面如下图所示。



CA的crl下载配置

下载类型: ldap

IP地址:

认证端口:

ldap服务器查询根键:

用户名:

密码:

确定 取消

各参数说明请参见下表。

参数	说明
下载类型	使用 LDAP 或 HTTP 协议向第三方 CA 发送自动下载 CRL 请求。
IP 地址及认证端口	使用 LDAP 协议向第三方 CA 发送下载 CRL 请求时，指定 LDAP 服务器的 IP 地址（或域名）及查询端口号。
LDAP 服务器查询根键	设置 LDAP 服务器进行证书查找的根域，具体参照 LDAP 服务器的设置。

参数	说明
用户名及密码	指定登录 LDAP 服务器时使用的用户名和密码。

如果选择通过 HTTP 方式下载，界面如下图所示。



该界面标题为“CA的crl下载配置”。包含两个主要配置项：

- 下载类型**：一个下拉菜单，当前显示为“http”。
- url地址**：一个文本输入框，目前为空。

 界面底部有两个按钮：“确定”和“取消”。

其中，“URL 地址”是指当使用 HTTP 协议向第三方 CA 发送下载请求时，指向 CA 服务器 CRL 信息的链接。

参数设置完成后点击“确定”按钮即可。

3) 设置自动下载周期，以便安全网关定时自动下载更新 CRL 文件。

在“CA 证书维护”页面中，点击右上方的“配置 CRL 自动下载”，设置 CA 证书撤销列表文件更新周期，如下图所示。



该界面标题为“CRL自动下载”。包含一个配置项：

- 时间间隔**：一个文本输入框，当前值为“86400”，右侧带有“秒”单位。下方有提示文字：“[60~172800秒, 默认一天(86400秒)]”。

 界面底部有两个按钮：“确定”和“取消”。

参数设置完成后，点击“确定”按钮即可。

4) 即时下载 CRL 文件。

点击“CRL 下载”图标，安全网关立即从设定的 LDAP 服务器或 URL 地址上下载 CRL 文件。

12.3 本地 CA 策略

网络卫士安全网关内置了 CA 中心，企业或者事业单位可自建 CA 中心，用户可不必购买单独的 CA 认证体系，为企业减少了投入成本。内置 CA 的配置步骤为：

1) 管理员首先需要导入安全网关的根证书和私钥。请参见 [12.3.1配置内置CA根证书](#)

。

2) 证书发放及管理。管理员能够对设备或移动用户进行数字证书的发放、查看、导出、写入USBKey、撤销、删除等操作，还可以对CRL列表进行维护以对证书的有效性进行验证。请参见 [12.3.2签发证书](#)。

3) CRL列表维护。构建内置CA时导入CRL列表，证书撤销后重新发布CRL列表。请参见[12.3.3证书撤销列表设置](#)。

说明

- ✧ 如果使用CA签发的根证书和私钥对移动用户认证，管理员还需要导入CA证书，方法请参见[12.2.1配置CA根证书](#)。
- ✧ 对 VRC 客户端使用不同的认证方式时，在安全网关上的客户端设置将不同，具体请参见《TopGate 管理手册——IPSec VPN 配置》。

12.3.1 配置内置 CA 根证书

内置 CA 根证书和私钥可以通过以下几种方式导入：本地生成、使用安全网关的证书、导入其它 CA 签发的根证书和私钥。管理员可以设置内置 CA 的根证书，也支持内置 CA 根证书的导出功能，用于和第三方 CA 签发的证书进行交叉认证。

1. 导入内置 CA 根证书

具体步骤如下所示：

1) 在左侧导航菜单选择 **PKI设置 > 本地CA策略**，然后激活“根证书”页签，页面下方显示内置CA根证书信息，如下图所示。



2) 点击页面右上方的“获取证书”，可以导入内置 CA 根证书，界面如下图所示。

获取根证书

☒ 文件方式导入

证书 浏览...

私钥 浏览...

☐ PKCS12文件格式导入

证书文件 浏览...

证书文件密码

☐ 以本机设备证书导入

☐ 生成新证书

名称 *

国家 [两个英文字母]

省

城市

电子邮件

组织

单位

确定
取消

界面参数说明如下表所示：

参数	说明
文件方式导入	当内置 CA 根证书为上一级 CA 签发，且证书文件的证书文件和私钥文件分开存储时，需要分别设置证书和私钥文件在管理主机上的存放路径。
PKCS12 文件格式导入	当内置 CA 根证书为上一级 CA 签发，且证书文件采用 PKCS12 的格式存储时，需要设置证书文件的存放路径和证书文件的密码。
以本机设备证书导入	将本机证书作为内置CA根证书。关于本机证书的设置请参见 12.1本机证书 。 说明： 证书类型可以查看证书的“详细信息”页签中的“基本限制”一项，若 Subject Type=CA，则表示该证书为 CA 根证书。
生成新证书	安全网关作为根 CA 为自身生成一个新证书作为根证书。必须要设置证书的名称，其他属性为可选项。

3) 在选择好证书导入方式和正确输入相关的选项信息后，点击“确定”按钮，导入证书；点击“取消”，放弃导入。

证书导入成功后，将会在“客户端根证书”中显示新的证书信息。

说明

- ◇ 每台设备只能有一份客户端根证书用来生成移动用户所用的客户端证书。如果管理员导入第二份证书，将自动覆盖以前所导入的证书。
- ◇ 当更新客户端根证书后，以前发放的移动用户的客户端证书将全部失效，需要管理员重新为移动用户发放证书。

2. 导出 CA 根证书

安全网关支持以三种文件格式导出根证书：DER 格式、PEM 格式和 PKCS12 格式。

具体步骤如下所示：

1) 在左侧导航菜单选择 **PKI设置 > 本地CA策略**，然后激活“根证书”页签，页面下方显示内置CA根证书信息。

2) 点击页面右上方的“导出证书”，界面显示如下图所示。



导出根证书

选择要使用的文件格式

a) 选择导出的证书文件格式为“PKCS12”时，需要首先设定证书文件的密码（密码不输入时表示密码为空），如下图所示。

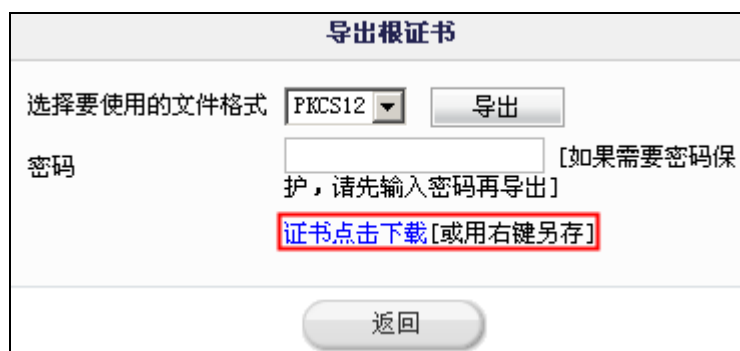


导出根证书

选择要使用的文件格式

密码
[如果需要密码保护，请先输入密码再导出]

然后点击“导出”按钮后，页面下方显示证书文件的下载链接，如下图所示。



导出根证书

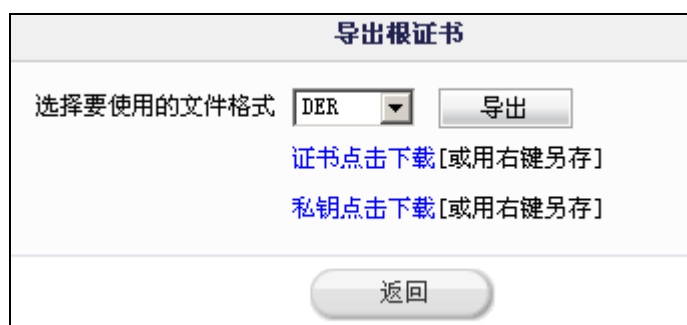
选择要使用的文件格式

密码 [如果需要密码保护，请先输入密码再导出]

[证书点击下载\[或用右键另存\]](#)

最后点击蓝色的“证书点击下载”链接，将该证书文件保存到管理主机上即可。

b) 选择的证书文件格式为“DER”或“PEM”时，点击“导出”按钮后，页面下方显示证书和私钥文件的下载链接，如下图所示。



点击蓝色的链接文字，然后分别将证书文件和私钥文件保存到管理主机上即可。

点击“返回”，系统跳转至根证书设置界面。

12.3.2 签发证书

安全网关内置 CA 的根证书导入后，安全网关即可为设备或移动用户签发证书，签发的证书采用证书名称来唯一标识证书。对于已经生成的证书，管理员可以查看证书属性、将证书导出到管理员所在主机上、将证书写入安全网关的 USBKey，也可以将证书撤销、删除或一次性清空。

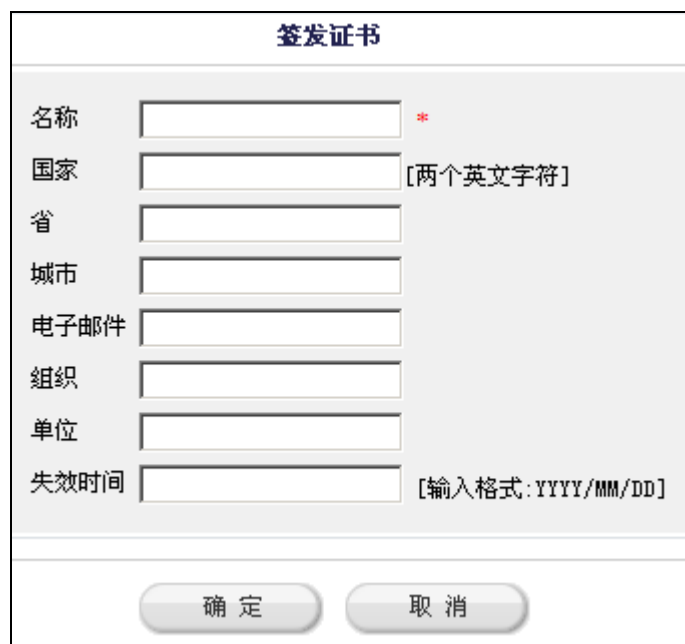
具体步骤为：

1) 在左侧导航菜单选择 **PKI设置 > 本地CA策略**，然后激活“签发证书”页签，页面中显示了安全网关内置CA签发的客户端证书，如下图所示。

根证书 签发证书 证书撤销列表								
生成新证书 全部导出 清空证书			总计: 3					
证书	有效起止日期	状态	属性	下载	写入	撤销	删除	
zhangsan	Jun 24 08:48:33 UTC 2010- Jun 21 08:48:33 UTC 2020	✓						
webui	Jun 24 08:47:58 UTC 2010- Jun 21 08:47:58 UTC 2020	✓						
doc	Jun 24 08:48:19 UTC 2010- Jun 21 08:48:19 UTC 2020	✓						

2) 签发证书

点击页面右上方的“生成新证书”，可以为客户端签发证书，如下图所示。



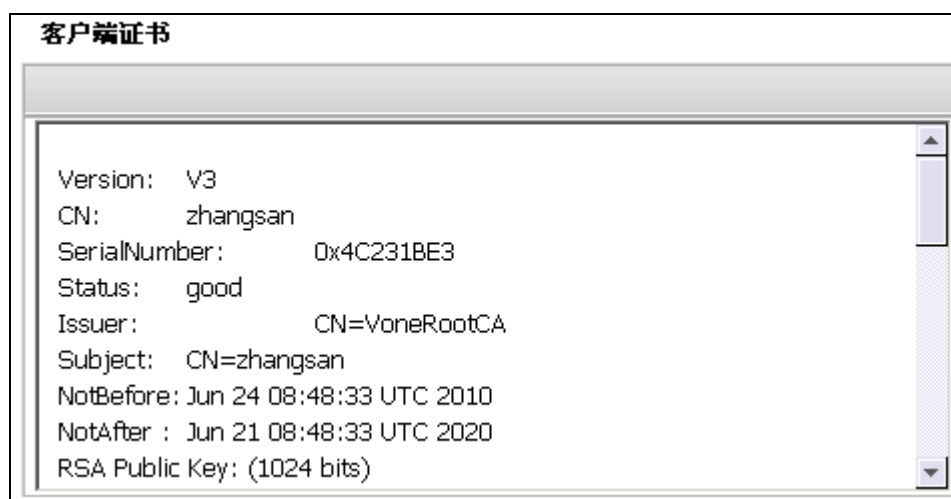
The image shows a '签发证书' (Issue Certificate) form. It contains several input fields: '名称' (Name) with a red asterisk indicating it is required; '国家' (Country) with a hint '[两个英文字符]' (2 English characters); '省' (Province); '城市' (City); '电子邮件' (Email); '组织' (Organization); '单位' (Unit); and '失效时间' (Expiration Time) with a hint '[输入格式: YYYY/MM/DD]' (Input format: YYYY/MM/DD). At the bottom are '确定' (OK) and '取消' (Cancel) buttons.

在“名称”处输入新证书的名称，该名称唯一地标识证书。国家、省、城市、电子邮件、组织、单位，以及证书的失效时间均为证书的属性字段，为可选输入项，管理员签发证书时可以不输入。

参数设置完成后，点击“确定”按钮，生成客户端证书。新生成的客户端证书信息将显示在客户端证书列表中。

3) 查看证书信息

点击客户端证书条目右侧的“属性”图标，可以查看该客户端证书的详细信息，如下图所示。



The image shows a '客户端证书' (Client Certificate) details window. It displays the following information: Version: V3; CN: zhangsan; SerialNumber: 0x4C231BE3; Status: good; Issuer: CN=VoneRootCA; Subject: CN=zhangsan; NotBefore: Jun 24 08:48:33 UTC 2010; NotAfter: Jun 21 08:48:33 UTC 2020; RSA Public Key: (1024 bits).

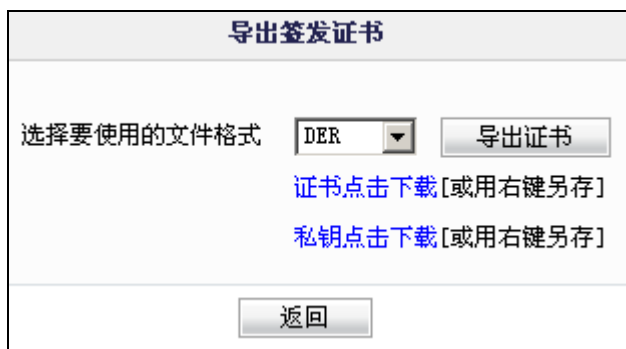
4) 下载证书

点击客户端证书条目右侧的“下载”图标，可以将安全网关的内置 CA 签发的客户端证书导出到管理员所在主机上。

a) 在客户端证书列表中，点击待下载证书条目后的“下载”图标，进入证书导出页面，如下图所示。

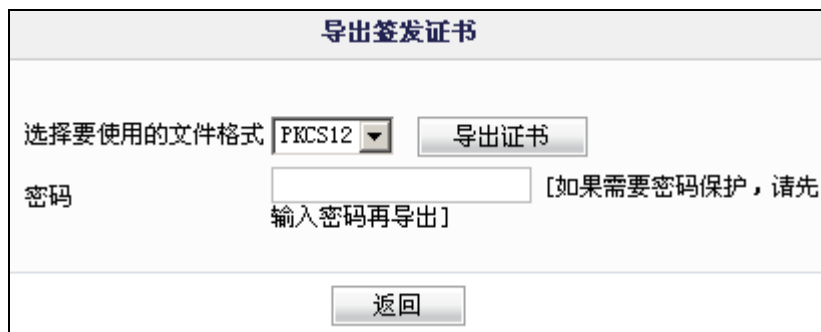


b) 选择导出的文件格式为“DER”或“PEM”时，点击“导出证书”按钮后，页面下方显示证书和私钥文件的下载链接，如下图所示。



点击蓝色的链接文字，然后分别将证书文件和私钥文件保存到管理主机上即可。

c) 选择导出的文件格式为“PKCS12”时，需要设定证书文件的密码（密码不输入时表示密码为空），如下图所示。



点击“导出证书”按钮后，页面下方显示证书文件的下载链接，如下图所示。

导出签发证书

选择要使用的文件格式

PKCS12

导出证书

密码

[如果需要密码保护，请先输入密码再导出]

证书点击下载

[或用右键另存]

返回

点击蓝色的“证书点击下载”链接，然后将该证书文件保存到管理主机上即可。

d) 选择导出的证书类型为“TAR”，然后点击“导出证书”按钮，页面下方显示 TAR 文件的下载链接（TAR 文件中包括打包的客户端证书、私钥和安全网关内置 CA 根证书），如下图所示。

导出签发证书

选择要使用的文件格式

TAR

导出证书

证书点击下载

[或用右键另存]

返回

点击蓝色的“证书点击下载”链接，然后将该 TAR 文件保存到管理主机上即可。

5) 写入证书到 USBKey

点击客户端证书条目右侧的“写入”图标，可以直接将证书写入到安全网关的 USBKey 中，如下图所示。

写入USB

USB厂商

epass1000

客户端用户名

webui

PIN码

确认PIN码

写入

取消

参数说明如下表所示：

参数	说明
USB 厂商	用于选择 USBKey 设备厂商/型号，该选项请根据插在安全设备上的不同 USBKey 进行选择。目前只支持 epass1000。

参数	说明
客户端用户名	显示为证书名称，管理员可以在导出时进行修改。
PIN 码	USBKey 的 PIN 码。
确认 PIN 码	再次输入 USBKey 的管理员 PIN 码。

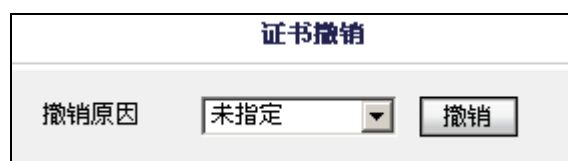
点击“写入”按钮，如果安全网关和 USBKey 的连接正确，可以将证书写入 USBKey 中；点击“取消”，放弃设置。

说明

- ✧ 在将客户端证书写入到USBKEY之前，安全网关设备上必须已经插入了USBKEY，同时必须保证安全网关设备的USBKey接口处于启用状态，具体设置请参见 [12.4USB KEY](#)。
- ✧ 错误输入 PIN 码次数过多可能造成 USBKey 死锁，死锁状态下的 USBKey 必须进行初始化方能正常使用。

6) 撤销证书

点击客户端证书条目右侧的“撤销”图标，可以将该证书撤销掉，如下图所示。



证书撤销对话框，包含撤销原因选择框（当前显示“未指定”）和撤销按钮。

撤销原因可以选择“未指定”、“密钥泄露”、“CA 密钥泄露”或“附属关系改变”。然后点击“撤销”按钮即可。证书被成功撤销后，该客户端证书的“状态”显示为“×”（“状态”图标显示为“√”表示该证书为有效证书，显示为“×”表示该证书为无效证书）。

说明

- ✧ 证书撤销后，需要管理员手动更新CRL列表，具体请参见[12.3.3证书撤销列表设置](#)。

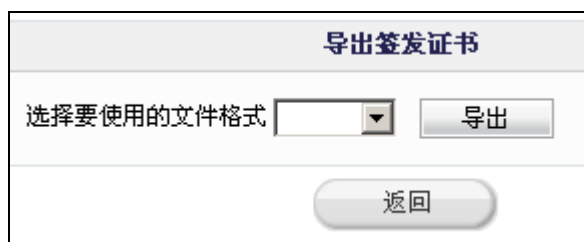
7) 删除客户端证书

点击待删除证书条目右侧的“删除”图标，可以删除该客户端证书文件。

8) 导出所有证书

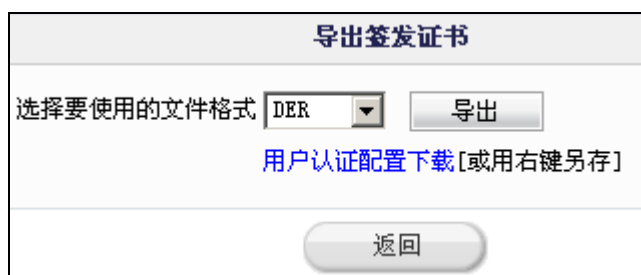
点击客户端证书列表左上方的“全部导出”，可以将安全网关签发的所有客户端证书一次性全部从安全网关上导出。

a) 点击“全部导出”，进入如下图所示页面。



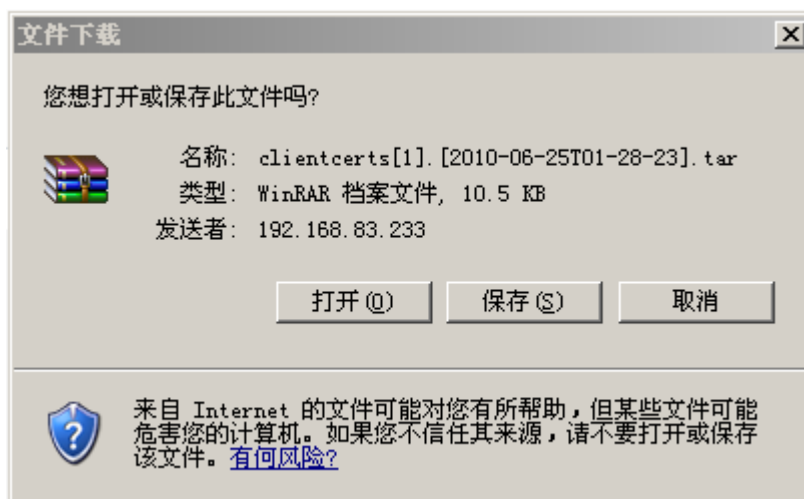
The dialog box is titled "导出签发证书" (Export Issued Certificate). It contains a label "选择要使用的文件格式" (Select the file format to use) followed by a dropdown menu and an "导出" (Export) button. At the bottom, there is a "返回" (Return) button.

b) 选择导出的文件格式为“DER”、“PEM”，点击“导出”按钮后，页面下方显示用户认证配置下载链接，如下图所示。



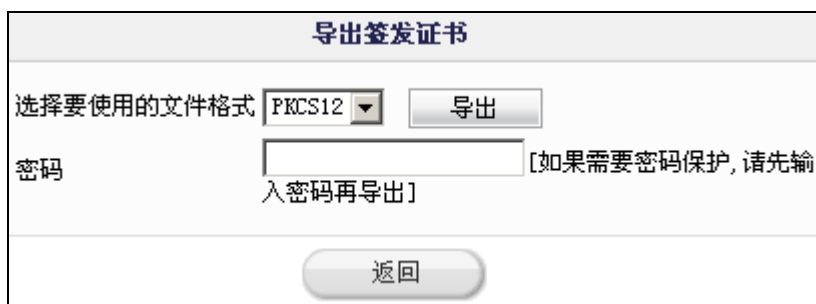
The dialog box is titled "导出签发证书" (Export Issued Certificate). The dropdown menu now shows "DER". Below the "导出" (Export) button, there is a blue link "用户认证配置下载" (Download User Authentication Configuration) with the text "[或用右键另存]" (or right-click to save as) in parentheses. At the bottom, there is a "返回" (Return) button.

点击蓝色字体“用户认证配置下载”链接，弹出如下图所示界面。



点击“保存”按钮完成证书导出。

c) 选择导出的文件格式为“PKCS12”，需要设定证书文件的密码（密码不输入时表示密码为空），如下图所示。



The dialog box is titled "导出签发证书" (Export Issued Certificate). The dropdown menu now shows "PKCS12". Below the "导出" (Export) button, there is a password input field with the label "密码" (Password) and the text "[如果需要密码保护, 请先输入密码再导出]" (If password protection is required, please enter the password before exporting). At the bottom, there is a "返回" (Return) button.

点击“导出”按钮后，页面下方显示证书文件的下载链接，如下图所示。

导出签发证书

选择要使用的文件格式

PKCS12

导出

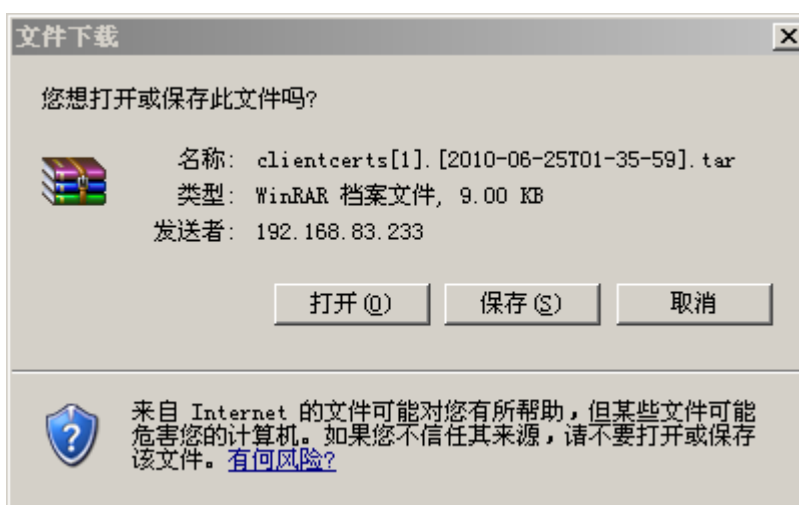
密码

[如果需要密码保护, 请先输入密码再导出]

[用户认证配置下载](#) [或用右键另存]

返回

点击蓝色字体的“用户认证配置下载”链接后，弹出如下图所示界面。



点击“保存”按钮完成证书文件导出。

d) 选择导出的证书类型为“TAR”，然后点击“导出”按钮，页面下方显示 TAR 文件的下载链接（TAR 文件中包括打包的客户端证书、私钥和安全网关内置 CA 根证书），如下图所示。

导出签发证书

选择要使用的文件格式

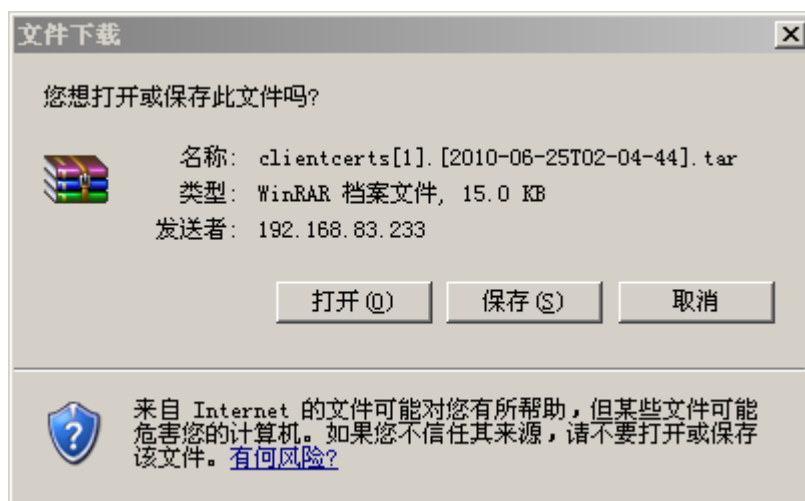
TAR

导出

[用户认证配置下载](#) [或用右键另存]

返回

点击蓝色字体的“用户认证配置下载”链接后，弹出如下图所示界面



点击“保存”按钮完成导出。

9) 清空证书

点击客户端证书列表右上方的“清空证书”，可以将安全网关签发的所有客户端证书一次性全部删除。

12.3.3 证书撤销列表设置

证书撤销列表 CRL 指定了所有被撤消的证书的唯一序列号。安全网关作为 CA 需要对 CRL 列表进行设置。包括两个方面：1) 支持 CRL 列表的导出功能，用于在隧道对端设备上导入 CRL 列表以验证证书有效性。2) 内置 CA 撤消不再被信赖的证书后，发布新的 CRL 列表信息。

具体操作步骤为：

1) 在左侧导航菜单选择 **PKI设置 > 本地CA策略**，然后激活“证书撤销列表”页签，页面中显示了上次发布的CRL列表信息，如下图所示。

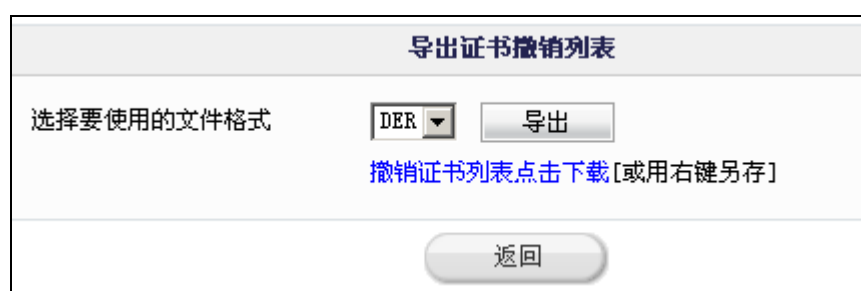


点击页面左上方的“发布新撤销列表”，则系统将更新文本框中的 CRL 列表信息。

点击页面左上方的“导出撤销列表”，可以将安全网关作为 CA 的 CRL 列表信息以 DER 或 PEM 格式导出到管理员所在主机上，界面如下图所示。



选择的证书文件格式：DER 格式或 PEM 格式，然后点击“导出”按钮，页面下方显示证书和私钥文件的下载链接，如下图所示。



点击蓝色的链接文字，将证书证书撤销列表文件保存到管理主机上即可。

12.4 USB KEY

网络卫士安全网关支持通过 USBKey 方式导入客户端或安全网关本机证书。由于出厂配置中，默认 USBKey 端口没有启动，因此，要想使用 USBkey 存储证书，还需要启用 USBKey 端口，并正确设置 USBKey 的厂商和 PIN 码。具体设置如下：

1) 点击 **PKI设置 > USB KEY**，界面如下图所示。



界面参数说明如下表所示。

参数	说明
USB 厂商	用于选择不同的 USBKey 设备提供厂商/型号。 目前只支持 epass1000；“none”表示不支持将设备签发的证书导入到 USBKey 中。
PIN 码	设置 USBKey 的 PIN 码。
确认 PIN 码	再次输入 USBKey 的 PIN 码。

2) 参数设置完成后，点击“应用”按钮，完成设置。

说明

✧ 错误输入 PIN 码次数过多可能造成 USBKey 死锁，死锁状态下的 USBKey 需返厂维修。

12.5 远程证书认证

当采用证书认证方式时，根据签发证书的 CA 是否是安全网关本身，分为本地证书认证、第三方 CA 离线认证、第三方 CA 在线认证三种。

本地证书认证和第三方 CA 离线认证均在网络卫士安全网关上对客户端证书进行认证，利用颁发者证书和证书撤销列表（CRL）来验证签名证书的有效性；当采用第三方 CA 在线认证方式时，网络卫士安全网关支持通过向 LDAP 服务器和 OCSP 服务器在线查询第三方 CA 签发的证书是否有效。具体设置如下所示：

1) 点击 **PKI设置 > 远程证书认证**。

2) 当选择“认证协议类型”为“LDAP”时，界面如下图所示。

远程证书认证

远程证书认证配置

远程证书认证

停用

协议类型

LDAP

服务器地址

服务器端口

查询根键

[例如: dc=base, dc=com]

用户帐号

用户密码

应用

各参数说明请参见下表。

参数	说明
支持远端证书认证	是否采用远端证书认证。 可选项为启用、停用。 默认为关闭状态，选择“启用”可以启动该功能。
认证协议类型	目前支持 LDAP 和 OCSP。
服务器地址	当选择“LDAP”时，用于设置 LDAP 服务器 IP 地址。
服务器端口	当选择“LDAP”时，用于设置 LDAP 服务器的服务端口，范围 1-65535。
查询根键	当选择“LDAP”时，用于设置服务器进行证书查找的根域，具体参照 LDAP 服务器的设置。例如：dc=topsec,dc=com。
用户帐号	当选择“LDAP”时，用于设置登录 LDAP 服务器的用户帐号名。
用户密码	当选择“LDAP”时，用于设置登录 LDAP 服务器用户的密码。
ocsp 服务器 URL	当选择“OCSP”时，用于设置 OCSP 服务器的 URL 地址。

3) 参数设置完成后，点击“应用”按钮即可。

12.6 证书请求

网络卫士安全网关提供了证书请求功能，可以通过生成证书请求文件的方式向第三方 CA 认证中心申请网关证书（包括 IPsec VPN 网关和 SSL VPN 网关），然后再导入到网络卫士安全网关中。导入的证书文件作为 IPsec VPN 网关或 SSL VPN 网关的本机证书，显示在 **PKI 设置 > 本机证书** 的“IPsec VPN”页签或“SSL VPN”页签中。

12.6.1 配置 IPsec VPN 证书请求

1) 点击导航树菜单 **PKI 设置 > 证书请求**，然后激活“IPsec VPN”页签，进入 IPsec VPN 网关证书请求页面，页面中显示了当前 IPsec VPN 网关的证书请求文件内容。



2) 点击“管理”，进入证书请求文件的管理界面，如下图所示。

The screenshot shows a web interface with two main sections. The top section, titled '导入证书' (Import Certificate), contains two radio buttons: 'PEM证书导入' (selected) and 'DER证书导入'. Each has a text input field and a '浏览...' (Browse...) button. Below these is a '提交' (Submit) button. The bottom section, titled '生成证书请求' (Generate Certificate Request), contains several form fields: '名称' (Name) with a red asterisk, '组织' (Organization), '机构名' (Institution Name), '国家名' (Country Name), '省' (Province), '区县' (District/County), '电子邮箱' (Email), '密钥长度' (Key Length) set to 1024, and '哈希算法' (Hash Algorithm) set to SHA1. A '生成' (Generate) button is at the bottom.

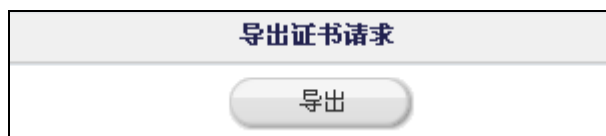
3) 生成证书请求

输入证书请求字段，包括名称、组织、机构名等信息，然后点击“生成”按钮，转入该证书请求内容的显示页面，如下图所示。

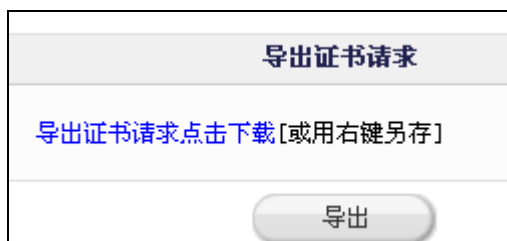
The screenshot shows a web interface with a tabbed header for 'IPsec VPN' and 'SSL VPN'. Below the tabs are '管理' (Manage) and '删除' (Delete) buttons. The main content area displays the details of a 'Certificate Request'. The data shown is: Version: 0 (0x0), Subject: CN=zhangsan ,OU=topsecdoc ,ST=bj ,C=cn, Subject Public Key Info: Public Key Algorithm: rsaEncryption, RSA Public Key: (1024 bit), Modulus (1024 bit): 00:b7:94:6f:12:57:af:f6:77:d1:e7:0d:95:b3:bb:4b:6f:3f:13:94:ff:56:00:89:79:3c:97:dc:a0:c6:.

4) 导出该证书请求文件

a) 点击“管理”链接，准备导出该证书请求文件，以便将其导入到第三方 CA 认证中心。



b) 在证书请求文件的管理界面中，点击“导出”按钮，页面下方显示证书请求文件的下载链接，如下图所示。



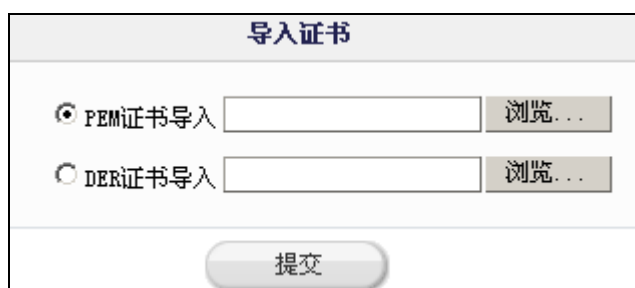
c) 点击蓝色的链接文字，然后将该证书请求文件保存到管理主机上。

此后，第三方 CA 将根据该证书请求文件为 IPsec VPN 网关签发网关证书。

5) 证书导入

即如何将已经成功签发的网关证书导入到网络卫士安全网关中。

a) 在 IPsec VPN 证书文件管理页面中，根据网关证书的文件格式勾选“PEM 证书导入”或“DER 证书导入”，如下图所示。



b) 然后点击“浏览...”按钮，选择第三方 CA 根据证书请求文件生成的网关证书。

网络卫士安全网关在生成证书请求的同时也生成了与公钥相对应的私钥文件，所以此处只需导入网关证书既可。

c) 点击“提交”按钮，既可将该IPsec VPN网关证书导入到网络卫士安全网关中。此时，可以通过点击导航树 **PKI设置 > 本机证书** 中的“IPsec VPN”页签进行查看。

12.6.2 配置 SSL VPN 证书请求

1) 点击导航树菜单 **PKI设置 > 证书请求**，然后激活“SSL VPN”页签，进入SSL VPN 网关证书请求页面，页面中显示了当前SSL VPN网关的证书请求文件内容。

2) 点击“管理”链接，进入证书请求文件的管理界面，如下图所示。

导入证书

☒ PEM证书导入

浏览...

☐ DER证书导入

浏览...

提交

生成证书请求

名称

*

组织

机构名

国家名

省

区县

电子邮箱

密钥长度

1024

▼

哈希算法

SHA1

▼

生成

3) 生成证书请求

输入证书请求字段，包括名称、组织、机构名等信息，然后点击“生成”按钮，转入该证书请求内容的显示页面，如下图所示。

IPsec VPN

SSL VPN

管理

删除

Certificate Request:

Data:

Version: 0 (0x0)

Subject: CN=sv_client

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

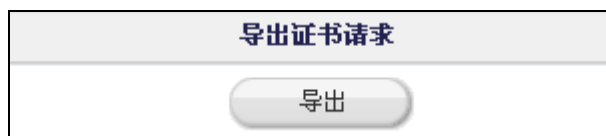
Modulus (1024 bit):

00:b0:41:9a:4e:3b:b5:0d:1b:37:74:a4:2a:71:38:

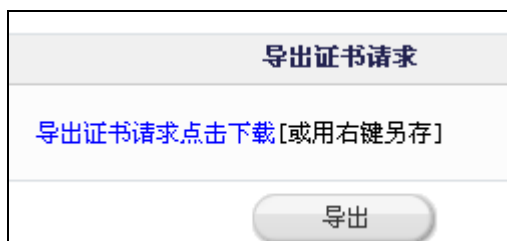
89:4d:02:5e:9f:38:ac:48:27:df:0d:b7:ab:9a:cf:

4) 导出该证书请求文件

a) 点击“管理”链接，准备导出该证书请求文件，以便将其导入到第三方 CA 认证中心。



b) 在证书请求文件的管理界面中，点击“导出”按钮，页面下方显示证书请求文件的下载链接，如下图所示。



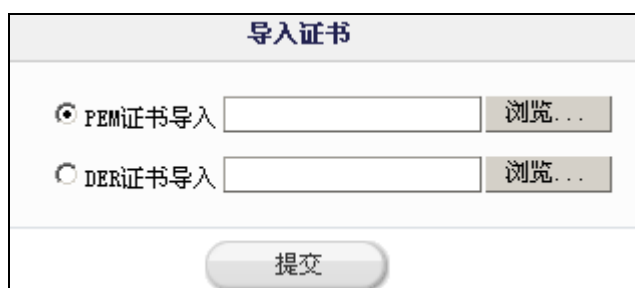
c) 点击蓝色的链接文字，然后将该证书请求文件保存到管理主机上。

此后，第三方 CA 将根据该证书请求文件为 SSL VPN 网关签发网关证书。

5) 导入证书

介绍如何将已经成功签发的网关证书导入到网络卫士安全网关中。

a) 在 SSL VPN 证书文件管理页面中，根据网关证书的文件格式勾选“PEM 证书导入”或“DER 证书导入”，如下图所示。



b) 然后点击“浏览...”按钮，选择第三方 CA 根据证书请求文件生成的网关证书。

网络卫士安全网关在生成证书请求的同时也生成了与公钥相对应的私钥文件，所以此处只需导入网关证书既可。

c) 点击“提交”按钮，既可将该SSL VPN网关证书导入到网络卫士安全网关中。此时，可以通过点击导航树 **PKI设置 > 本机证书** 中的“SSL VPN”页签进行查看。

12.7 备份和恢复

管理员可以对安全网关中保存的证书文件进行维护，包括证书文件的恢复和下载功能。

说明

- ◇ 备份证书时是对 flash 上保存证书目录中的证书进行下载。如果在创建证书后没有保存配置，创建的证书文件不会存放在证书保存目录中，如果这时进行备份无法下载所有证书文件。

维护配置的操作方法如下：

- 1) 选择 **PKI管理 > 备份和恢复**，出现如下页面。

备份和恢复	
证书文件恢复	
证书文件位置	浏览...
上传证书	
证书文件下载	
下载证书	下载证书

- 2) 证书文件恢复

点击“浏览”，选择配置文件所在的目录，点击“上传证书”，则将本地保存的证书文件加载到设备上。在进行证书恢复时，设备上原有的所有证书文件都会被删除。

- 3) 下载证书文件

管理员可以一次性导出系统所有证书文件，保存在管理主机指定目录中进行备份。

点击“下载证书”，此时界面上增加“系统所有证书下载”的链接，如下图。

证书文件下载	
下载证书	下载证书
系统所有证书下载 [或用右键另存]	

点击蓝色链接，或点击鼠标右键菜单中选择“目标另存为”，可以将证书文件保存到管理主机本地的文件夹中。

需要注意的是，备份证书是对flash上保存证书目录中的证书进行下载。如果在创建证书后没有保存配置，创建的证书文件不会存放在证书保存目录中，如果这时进行备份无法下载所有证书文件。

13 虚拟专网

虚拟专网（VPN，Virtual Private Network），被定义为通过一个公用网络（通常是因特网）建立的一个临时的、安全的连接，就像一条穿过非安全网络的安全、稳定的隧道，对所传输的数据进行加密保护。虚拟专用网可以帮助远程用户、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。

天融信网络卫士安全网关提供完备的 VPN 连接功能，可以支持隧道的负载均衡，GRE over IPSec，动态路由 OSPF 穿越隧道，组播穿越隧道以及隧道流量统计等。网络卫士安全网关支持利用标准的 IKE 和 IPSec 协议，与天融信的 IPSec VPN 以及其他支持 IKE 标准协议的 VPN 网关设备协商并建立标准的 IPSec VPN 隧道，关于 IPSec VPN 的配置请参考《TopGate 管理手册——IPSEC VPN 配置》。

本章主要介绍网络卫士安全网关作为 VPN 网关设备的配置和管理，主要内容包括：

- L2TP 管理。主要介绍如何利用 L2TP 协议建立远端用户与网络卫士安全网关之间的 VPN 连接。
- PPTP 管理。主要介绍如何利用 PPTP 协议建立远端用户与网络卫士安全网关之间的 VPN 连接。
- GRE 管理。主要介绍如何利用 GRE 协议与远端设备建立 GRE 隧道进行数据传输。

13.1 L2TP 管理

网络卫士安全网关不仅支持客户端通过标准的 IPSec 协议与安全网关建立 VPN 连接，而且支持 L2TP 协议。远端用户需要安装 Windows 自带的拨号连接组件，同时安装一个 TOPSEC 提供的小程序（该程序在安全网关随机光盘 tools 目录下和 TOPSEC 的网站上均可获取），以便与网络卫士安全网关通过 L2TP 服务建立连接，从而访问整个网络。

L2TP 客户端要通过安全网关的本地认证后才能与安全网关建立 L2TP 隧道，以安全访问内网资源，基础设置包括：

- 1) 在 **用户认证 > 用户管理** 中，添加 L2TP 用户，具体请参见 [8.1.1.1 配置用户](#)；然后将该用户添加到一个角色中，具体请参见 [8.2 用户角色设置](#)。
- 2) 在安全网关上开放客户机所属区域的 L2TP 服务，具体请参见 [4.2.2.2 开放服务](#)。
- 3) 设置客户机连接的安全网关接口区域属性应当为允许用户访问，具体请参见 [7.2 设置区域资源](#)。
- 4) 设置远程 L2TP 客户端可以访问的内网资源。通过添加访问控制规则，规则源设定为与属性“l2tp”（系统内置）绑定的区域来完成，具体请参见 [9.2.5 添加规则](#)。

5) 配置 L2TP 服务器参数 L2TP 连接服务的虚拟 IP 地址，并设置 IP 地址池以便为访问的客户端分配 IP 地址，具体操作请参见本节内容。

配置 L2TP 服务器参数的方法为：

1) 选择 **虚拟专网 > L2TP**，界面如下图所示。

界面参数说明如下表所示。

参数	说明
本地地址	L2TP 服务器的虚拟服务器 IP 地址，客户端将通过此地址与服务器通信。
起始地址/结束地址	L2TP 服务器地址池，服务器将为客户端动态分配此范围内的 IP 地址。必须和服务器的虚拟 IP 在同一个网段。设置与内网资源相同的子网段容易造成地址冲突，不建议这样设置。
要求数据加密	指定安全网关作为 L2TP 服务器是否要求使用数据加密。 说明： L2TP 服务器端和客户端的设置应当一致。
L2TP 状态	查看当前的 L2TP 连接状态信息。

2) 设置完参数后，用户需要首先点击“应用”按钮，然后再点击“启用”按钮，才能成功启动 L2TP 服务，在“L2TP 状态”框中可以查看当前的连接信息。

3) L2TP 用户通过安全网关的本地认证后，与安全网关建立一条 L2TP 隧道，状态信息如下图所示。

L2TP

L2TP设定

本地地址

50.0.0.1 *

起始地址

50.0.0.100 *

结束地址

50.0.0.200 *

☐ 要求数据加密

应用

启用

停止

L2TP状态

原始地址	指派地址
192.168.83.220	50.0.0.100

隧道总数: 1

L2TP认证用户和安全网关建立连接后可以通过菜单 **用户认证 > 用户管理** 的“在线用户”页签中查看。

用户管理

在线用户

用户设置

总计: 1

用户名	地址	服务器	登录时间(HH:MM:SS)	类型	删除此地址	删除此用户
lp	50.0.0.100	localdb	0:12:15	l2tp	-	-

说明

- ✧ 在 L2TP 客户端主机上, 必须首先运行小程序  **L2TP.exe**, 选中“允许 TOS 到 L2TP 的连接”, 点击“确定”按钮后重启客户端主机, 否则隧道无法建立成功。

13.2 PPTP 管理

网络卫士安全网关不仅支持客户端通过标准的 IPSec 协议与安全网关建立 VPN 连接, 而且支持 PPTP 协议, 远端用户可通过 Windows 自带的拨号连接组件与网络卫士安全网关通过 PPTP 服务建立连接, 从而访问整个网络。

PPTP 客户端需要通过安全网关的本地认证后才能与安全网关建立 PPTP 隧道, 以安全访问内网资源, 相关设置包括:

- 1) 在 **用户认证 > 用户管理** 中, 添加PPTP用户, 具体请参见 [8.1.1.1配置用户](#); 然后将该用户添加到一个角色中, 具体请参见 [8.2用户角色设置](#)。
- 2) 在安全网关上开放客户机所属区域的PPTP服务, 具体请参见[4.2.2.2开放服务](#)。

3) 设置客户机连接的安全网关接口区域属性应当为允许用户访问，具体请参见[7.2设置区域资源](#)。

4) 设置远程PPTP客户端可以访问的内网资源。通过添加访问控制规则，规则源设定为与属性“pptp”（系统内置）绑定的区域来完成。也可以通过包含PPTP用户的角色设置访问控制规则来对PPTP客户端进行访问控制。具体请参见[9.2.5添加规则](#)。

5) 配置 PPTP 连接服务的虚拟 IP 地址和端口信息，并设置 IP 地址池以便为访问的客户端分配 IP 地址，具体操作请参见本节如下内容。

设置 PPTP 的具体方法为：

1) 选择 **虚拟专网 > PPTP**，界面如下图所示。

界面参数说明如下表所示。

参数	说明
本地地址	PPTP 服务器的虚拟服务器 IP 地址，客户端将通过此地址与服务器通信。
起始地址/结束地址	PPTP 服务器地址池，服务器将为客户端动态分配此范围内的 IP 地址。必须和服务器的虚拟 IP 在同一个网段。设置与内网资源相同的子网段容易造成地址冲突，不建议这样设置。
要求数据加密	指定 PPTP 服务器是否要求使用数据加密。 说明： PPTP 服务器端和客户端的设置应当一致，否则无法认证成功。 在 PPTP 客户端连接的属性窗口中，点击“安全”页签。 A) 如果选择“典型配置”，则下方的“要求数据加密”选项应当和 PPTP 服务器端一致； B) 如果选择“高级”，在“高级安全设置”窗口中，当“数据加密”选项选择“不允许加密”和“可选加密”时，在“允许这些协议”处不能选择“Shiver 密码身份验证协议”，此时安全网关上的 PPTP 服务器参数中不能勾选“要求数据加密”；当“数据加密”选项选择“需要加密”和“最大强度的加密”时，在“允许这些协议”处必须选择“MS-CHAP”、“允许为 Windows95 使用旧版 MS-CHAP”和

参数	说明
	“MS-CHAPV2”中的至少一项，此时安全网关上的 PPTP 服务器参数中必须勾选“要求数据加密”。
PPTP 状态	查看当前的 PPTP 连接状态信息。

2) 设置完参数后，用户需要首先点击“应用”按钮，然后再点击“启用”按钮，才能成功启动 PPTP 服务，在“状态”框中可以查看当前的连接信息。

3) PPTP 用户通过安全网关的本地认证后，与安全网关建立一条 PPTP 隧道，状态信息如下图所示。

PPTP 认证用户和安全网关建立连接后可以通过菜单 **用户认证 > 用户管理** 的“在线用户”页签中查看。

用户管理 在线用户 用户设置						
						总计: 1
用户名	地址	服务器	在线时间(HH:MM:SS)	类型	删除此地址	删除此用户
user_pptp	20.0.0.10	localdb	0:1:5	pptp	-	-

13.3 GRE 管理

GRE (Generic Routing Encapsulation, 通用路由封装) 协议是对某些网络层协议 (如 IP 和 IPX) 的数据报进行封装, 使这些被封装的数据报能够在另一个网络层协议 (如 IP) 中传输。GRE 是 VPN (Virtual Private Network) 的第三层隧道协议, 在协议层之间采用了一种被称之为 Tunnel (隧道) 的技术。Tunnel 是一个虚拟的点对点的连接, 在实际中

可以看成仅支持点对点连接的虚拟接口，这个接口提供了一条通路使封装的数据报能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报进行封装及解封装。

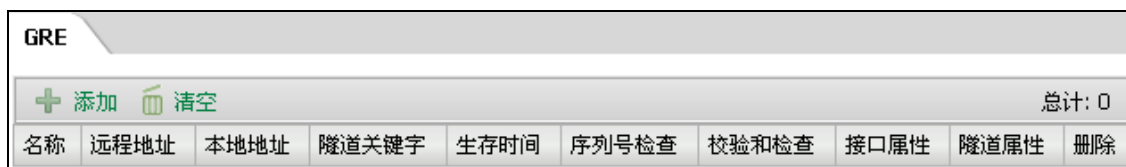
网络卫士安全网关不仅支持 GRE（Generic Routing Encapsulation）协议，实现与 Cisco 设备之间建立 GRE 隧道，而且支持 GRE 隧道与 IPSec 隧道的绑定（GRE over IPSec）以及 GRE 隧道内流量的负载均衡。

说明：

- ✧ 要使 OSPF 路由信息通过 GRE 隧道转发，就必须为 GRE 虚接口设置 IP 地址，然后指定 GRE 虚接口所在网段运行 OSPF 协议，具体请参见 [6.4.3.4 设置区域](#)。
- ✧ GRE 隧道与 IPSec 隧道的绑定设置，需要在添加静态隧道时在第二阶段协商的高级参数中启用“GRE 隧道关联”，并选择定义的 GRE 隧道名，具体设置请参见《TopGate 管理手册——IPSec 配置》。

在安全网关上需要设置 GRE 隧道的参数，设置方法如下所示：

1) 点击左侧导航树 **虚拟专网 > GRE**，界面如下图所示。



2) 点击“添加”，设置 GRE 隧道参数，界面如下图所示。

GRE 隧道

名称	gre-	*隧道名称必须以 gre- 开头
远程地址		*
本地地址		*
隧道关键字		[0-4294967295]
隧道生存时间		[1-255]
校验和检查	☐ 开启	
序列号检查	☐ 开启	

界面参数说明如下表所示。

参数	说明
名称	隧道名称，必须以“gre-”作为开头。建议使用 gre-加 0 到 1023 之间的数字来为 GRE 虚接口命名，例如 gre-0。

参数	说明
远程地址	隧道对端接收 GRE 报文的实际物理接口的 IP 地址。
本地地址	隧道本地发出 GRE 报文的实际物理接口的 IP 地址。
隧道关键字	可选项，标示隧道关键字，作为验证隧道有效性的依据。隧道两端配置的 KEY 必须一致，否则无法通过验证。 取值范围：0-4294967295。
隧道生存时间	可选项，设置允许隧道生存的时间。 取值范围：1-255。
校验和检查	可选项，设置是否开启校验和检查。如果开启校验和检查功能，则发送方将对 GRE 头及报文负载计算校验和，接收方对接收到的报文计算校验和并与报文中的校验和进行比较，一致则对报文进一步处理，否则丢弃。 on: 开启；off: 关闭。默认为 off。 说明： 如果只有隧道一端配置了使用校验和，将不对报文进行校验和检验；只有隧道两端都配置了开启“校验和检查”功能，才对报文进行校验和检验。
序列号检查	可选项，设置是否开启序列号检查。开启后，收发双方将进行序列号同步，只有对同步的报文才进行进一步处理，否则将报文丢弃。 on: 开启；off: 关闭。默认为 off。 说明： 只有在通道两端同时开启或关闭序列号同步机制时，通道才能建立。

4) 设置参数后，点击“确定”按钮，新添加的 GRE 隧道参数会显示在界面中。

添加GRE隧道后，会自动在安全网关上添加同名的虚拟GRE接口，需要管理员在 WEBUI界面或命令行下添加该接口的路由信息后，数据报文才会通过GRE隧道，具体设置请参见 [6.4.1路由表](#)。

例如新添加 gre-0 隧道，如果管理员要求通过 gre-0 隧道和目的网段 192.168.95.0/24 的通信，添加路由命令为：

```
#network route add dst 192.168.95.0/24 dev gre-0
```

5) 设置 GRE 虚接口属性。

点击某策略的“接口属性”图标，界面如下图所示。

接口设置

名称

gre-doctest

状态

☐ 停用

接口地址

地址

掩码

添加

地址

掩码

删除

确定

取消

界面参数说明如下表所示。

参数	说明
状态	设置 GRE 虚接口的状态。默认为“打开”状态；如选择“关闭”，则该虚接口将不会工作。
接口地址	定义 GRE 虚接口的 IP 地址。在右侧文本框中输入接口地址和掩码后，点击“添加”按钮即可。 说明： 要使 OSPF 路由信息通过 GRE 隧道转发，就必须为 GRE 虚接口设置 IP 地址，然后指定 GRE 虚接口所在网段运行 OSPF 协议，具体请参见 6.4.3.4 设置区域 。

参数设置完成后，点击“确定”按钮即可。

6) 修改隧道参数。

点击待修改策略条目右侧的“隧道属性”图标，可以修改已添加隧道部分参数。

7) 删除隧道。

点击该隧道的“删除”图标，可以删除该 GRE 隧道。

点击“清空”一次删除所有隧道。

14 入侵防御

网络卫士安全网关内置了 IDS 模块，可以为安全网关及其所保护网络内的主机提供简单的抗网络攻击的功能。同时，网络卫士安全网关可以实现与其他厂商入侵检测系统的联动，对用户内部网络提供了全面、高效的安全保护。

本章内容主要包括：

- 主机防护。介绍网络卫士安全网关为所有主机提供的主机防护功能。
- 主机限制。介绍安全网关为所有主机提供的主机限制功能。
- Anti-DOS。介绍网络卫士安全网关可以检测并抵御的常见攻击类型并设置 IDS 规则。
- 防 ARP 欺骗。介绍防 ARP 欺骗的设置，以防止局域网内的某些计算机冒充网关设备的 IP 地址发送 ARP 信息，导致正常计算机无法访问设备或外网。
- 防路由欺骗。介绍如何开启接口路由的反向路径查询功能，以有效防止基于源地地址欺骗的网络攻击行为。
- IDS 联动。介绍网络卫士安全网关同其它 IDS 产品联动的设置。

14.1 主机防护

主要介绍为主机对象、范围对象和子网对象设置防护功能。

14.1.1 主机防护

网络卫士安全网关为所有已经配置的主机对象提供了主机防护功能，用户可以通过设置 SYN 代理、最大报文长度来保证被保护主机的正常工作。

设置主机防护的具体步骤如下：

1) 选择 **入侵防御 > 主机防护**，然后激活“主机防护”页签，用户可以看到被保护主机，如下图所示。

主机防护 范围防护 子网防护					
					总计: 13
主机地址	SYN代理	最大报文长度	SYN攻击数	ACK攻击数	操作
server1	关		0	0	
host1	关		0	0	
server2	关		0	0	
WebServer1	关		0	0	
WebServer2	关		0	0	
WebServer	关		0	0	

默认情况下，安全网关系统对其所有的“主机对象”都提供主机防护功能，但是需要用户根据具体情况为各主机设置不同的防护参数。

2) 点击待修改主机防护信息条目后的“修改”图标，可以修改该主机的各防护参数，如下图所示。

防护主机属性

名称

SYN代理

最大报文长度 [63-4314, 默认值1460]

图中各参数的具体说明如下表。

参数	说明
名称	显示防护主机的对象名称。 用户无法修改该参数。
SYN 代理	是否启用 SYN 代理，以预防针对该主机的 SYN Flood 攻击。 可选值：开、关。
最大报文长度	设置最大报文段长度（MSS，即 TCP 层能够发送的数据块最大长度，此长度不包括 TCP 头内容），超过该长度后会进行分片。 说明： 只有当开启了 SYN 代理之后，才能够设置该参数值。

3) 参数设置完成后，点击“确定”按钮即可。

14.1.2 范围防护

网络卫士安全网关为所有已经配置的范围对象提供了防护功能，用户可以通过设置 SYN 代理和最大报文长度来保证被保护范围中主机的正常工作。

设置范围防护的具体步骤如下：

1) 选择 **入侵防御 > 主机防护**，然后激活“范围防护”页签，用户可以看到被保护主机范围，如下图所示。

主机防护 范围防护 子网防护					
					总计: 2
范围名称	SYN代理	最大报文长度	SYN攻击数	ACK攻击数	操作
any	关		0	0	
研发中心	关		0	0	

默认情况下，安全网关系统对其所有的“范围”对象都提供范围防护功能，但是需要用户根据具体情况为各范围设置不同的防护参数。

2) 点击待修改范围防护信息条目后的“修改”图标，可以修改该范围的各防护参数，如下图所示。

防护范围属性

名称

SYN代理

关

▼

最大报文长度

[63-4314, 默认值1460]

确定

取消

图中各参数的具体说明如下表。

参数	说明
名称	显示防护范围的对象名称。 用户无法修改该参数。
SYN 代理	是否启用 SYN 代理，以预防针对该范围中所有主机的 SYN Flood 攻击。 可选值：开、关。
最大报文长度	设置最大报文段长度（MSS，即 TCP 层能够发送的数据块最大长度，此长度不包括 TCP 头内容），超过该长度后会进行分片。 说明： 只有当开启了 SYN 代理之后，才能够设置该参数值。

3) 参数设置完成后，点击“确定”按钮即可。

14.1.3 子网防护

网络卫士安全网关为所有已经配置的子网对象提供了防护功能，用户可以通过设置 SYN 代理和最大报文长度来保证被保护子网中主机的正常工作。

设置子网防护的具体步骤如下：

1) 选择 **入侵防御 > 主机防护**，然后激活“子网防护”页签，用户可以看到被保护子网信息，如下图所示。

子网防护					
					总计: 3
子网名称	SYN代理	最大报文长度	SYN攻击数	ACK攻击数	操作
10.10.10.0	关		0	0	
子网10.x	关		0	0	
rd_group	关		0	0	

默认情况下，安全网关系统对其所有的“子网”对象都提供防护功能，但是需要用户根据具体情况为各子网设置不同的防护参数。

2) 点击待修改子网防护信息条目后的“修改”图标，可以修改该子网的各防护参数，如下图所示。

防护子网属性

名称

SYN代理

最大报文长度 [63-4314, 默认值1460]

图中各参数的具体说明如下表。

参数	说明
名称	显示防护子网的对象名称。 用户无法修改该参数。
SYN 代理	是否启用 SYN 代理，以预防针对该子网的 SYNflood 攻击。 可选值：开、关。
最大报文长度	设置最大报文段长度（MSS，即 TCP 层能够发送的数据块最大长度，此长度不包括 TCP 头内容），超过该长度后会进行分片。 说明： 只有当开启了 SYN 代理之后，才能够设置该参数值。

3) 参数设置完成后，点击“确定”按钮即可。

14.2 主机限制

对于通过设备的新建连接，在进行目的 NAT 转换之后，访问控制规则处理之前，将对地址对象的连接数进行控制，如果超过设定的值，后续报文将全部丢弃。

说明

- 当防护主机同时属于某个范围或子网时，根据最先配置的资源中的并发连接数和并发半连接数对该主机进行控制。用户可以在命令行下通过 **define** 命令查看相应资源的ID号。

14.2.1 主机限制

网络卫士安全网关为所有已经配置的主机对象提供了主机限制功能，用户可以通过设置并发连接数、并发半连接数来保证被保护主机的正常工作。

设置主机限制的具体步骤如下：

1) 选择 **入侵防御 > 主机限制**，然后激活“主机限制”页签，用户可以看到被保护主机，如下图所示。

主机限制					
范围限制		子网限制			
					总计: 13
主机地址	并发连接数	并发半连接数	每秒新建连接上限	限制	操作
server1	0	0	0		
host1	0	0	0		
server2	0	0	0		
WebServer1	0	0	0		
WebServer2	0	0	0		
WebServer	0	0	0		

默认情况下，安全网关系统对其所有的“主机对象”都提供主机限制功能，但是需要用户根据具体情况为各主机设置不同的参数。

2) 点击待修改主机限制信息条目后的“修改”图标，可以修改该主机的各参数，如下图所示。

主机限制		范围限制	子网限制
限制主机属性			
名称	doc_webs		
并发连接数	0		
并发半连接数	0		
每秒新建连接上限	0		
限制	来源		
确定		取消	

图中各参数的具体说明如下表。

参数	说明
名称	显示防护主机的对象名称。用户无法修改该参数。
并发连接数	同一时刻，允许其它主机与该主机建立的最大连接数。
并发半连接数	同一时刻，允许其它主机与该主机建立的最大半连接数。 说明： 限制半连接主要是为了限制特定 IP 连续发 syn 包的个数，限制此 IP 对其他机器进行 syn 攻击。
每秒新建连接上限	指其他主机与该主机之间的每秒最大新建连接数。 取值范围：0-100000；缺省值：0。
限制	可选值：来源、目的。 当选择“来源”时，表示防护主机访问其他主机时进行限制；当选择“目的”时，表示其他主机访问防护主机时进行限制。

3) 参数设置完成后，点击“确定”按钮即可。

14.2.2 范围限制

网络卫士安全网关为所有已经配置的范围对象提供了范围限制功能，用户可以通过设置并发连接数来保证被保护范围中主机的正常工作。

设置范围限制的具体步骤如下：

1) 选择 **入侵防御 > 主机限制**，然后激活“范围限制”页签，用户可以看到被保护主机范围，如下图所示。

主机限制	范围限制	子网限制		
总计: 1				
范围名称	并发连接数	每秒新建连接上限	限制	操作
any	0	0		

默认情况下，安全网关系统对其所有的“范围”对象都提供范围限制功能，但是需要用户根据具体情况为各范围设置不同的参数。

2) 点击待修改范围限制信息条目后的“修改”图标，可以修改该范围的各参数，如下图所示。

图中各参数的具体说明如下表。

参数	说明
名称	显示对象名称。用户无法修改该参数。
并发连接数	同一时刻，允许其它主机与该范围内主机建立的最大连接数。 说明： 指该范围内每台主机的并发连接数。
每秒新建连接上限	指其它主机与该范围内某台主机之间的每秒最大新建连接数。 取值范围：0-100000；缺省值：0。
限制	可选值：来源、目的。 当选择“来源”时，表示该范围内的主机访问其他主机时进行限制； 当选择“目的”时，表示其他主机访问该范围内的主机时进行限制。

3) 参数设置完成后，点击“确定”按钮即可。

14.2.3 子网限制

网络卫士安全网关为所有已经配置的子网对象提供了子网限制功能，用户可以通过设置并发连接数来保证被保护子网中主机的工作。

设置子网限制的具体步骤如下：

1) 选择 **入侵防御 > 主机限制**，然后激活“子网限制”页签，用户可以看到被保护子网信息，如下图所示。

子网限制				
				总计: 1
子网名称	并发连接数	每秒新建连接上限	限制	操作
subn_doc	0	0		

默认情况下，安全网关系统对其所有的“子网”对象都提供限制功能，但是需要用户根据具体情况为各子网设置不同的参数。

2) 点击待修改子网限制信息条目后的“修改”图标，可以修改该子网的各参数，如下图所示。

主机限制	范围限制	子网限制
限制子网属性		
名称	subn_doc	
并发连接数	0	
每秒新建连接上限	0	
限制	来源	
确定 取消		

图中各参数的具体说明如下表。

参数	说明
名称	显示对象名称。用户无法修改该参数。
并发连接数	同一时刻，允许其它主机与该子网内主机建立的最大连接数。 说明： 指该子网内每台主机的并发连接数。
每秒新建连接上限	指其它主机与该子网内某台主机之间的每秒最大新建连接数。 取值范围：0-100000；缺省值：0。
限制	可选值：来源、目的。 当选择“来源”时，表示该子网内的主机访问其他主机时进行限制； 当选择“目的”时，表示其他主机访问该子网内的主机时进行限制。

3) 参数设置完成后，点击“确定”按钮即可。

14.3 Anti-DOS

网络卫士安全网关内置的 IDS 模块，可以有效检测并抵御常见的攻击行为，用户通过简单设置即可保护指定的网络对象免于受到以下类型的攻击：（1）统计型攻击，包括：SYN Flood、UDP Flood、ICMP Flood、IP Sweep 和 Port Scan。（2）异常包攻击，包括：

Land、Smurf、Ping of Death、WinNuke、TCP Scan、IP Option、TearOfDrop 和 Targa3。

下面详细介绍如下内容：

- 设置 IDS 规则：设置异常包攻击和统计型攻击的 IDS 规则。
- 攻击防护设置：设置统计类攻击的黑白名单。
- 攻击统计显示：查看攻击统计结果。

14.3.1 设置 IDS 规则

通过配置 IDS 规则，并且在访问控制规则中引用该规则，网络卫士安全网关可以实现对统计型攻击和异常包攻击的防护功能。对匹配 ACL 规则的数据包，将按照所引用的 IDS 规则的配置，保护设定的“目的地址对象”免于受到攻击。对于不同的流量，通过引用不同的 IDS 规则，可以配置不同的防护策略。

IDS 规则设置方法为：

- 1) 选择 **入侵防御 > Anti-DOS**，并激活“IDS规则”页签，如下图所示。

IDS规则			
黑白名单		攻击统计	
+ 添加 清空		总计: 1	
名称	攻击类型	日志	操作
rule_ids1	land pingofdeath targa3 icmpredrt teardrop	不记录	 

- 2) 添加 IDS 规则

- a) 点击“添加”，界面如下图所示。

编辑IDS规则

名称 *

日志记录 ☐

异常包攻击

☒ Land

☒ PingOfDeath

☒ Teardrop

☒ Targa3

☐ ipspoof

☒ icmpredrt

☐ Smurf

☐ Winnuke

☐ TcpScan

☐ IpOption

统计型攻击

名称	☐ 启动	阈值
SynFlood	☐	500
UdpFlood	☐	1000
IcmpFlood	☐	1000
IpSweep	☐	10
PortScan	☐	10

参数说明如下表：

参数	说明
名称	输入规则名称。
日志记录	设置是否开启日志开关。在设置完统计型攻击防护和异常包攻击防护后，
异常包攻击	选择安全网关可以防御的异常包攻击防护类型，包括：Land、Smurf、Ping of Death、WinNuke、TCP Scan、IP Option、Teardrop 和 Targa3。网络卫士安全网关只检测已选择的攻击类型。 说明： 1) Land，一种拒绝服务攻击。它使用伪造的 SYN 包，包的源地址和目标地址都被设置成被攻击方的地址，这样被攻击方会给自己发送 SYN-ACK 消息并发回 ACK 消息，创建一个空连接，每一个这样的连接都将保持到超时为止，这样过多的空连接会耗尽被攻击方的资源，导致拒绝服务。 2) Smurf 是一种拒绝服务攻击，简单的来说，它可以通过大规模的发送以被攻击方的 IP 地址为源地址，以一个具有大量主机的网络广播地址为目的地址的 ICMP 请求包，这样大量的 ICMP 回复包将会耗尽被攻击方的资源，导致拒绝服务的发生。 3) Ping of Death 是一种拒绝服务攻击，通过向被攻击方发送超大的 ICMP 包，造成被攻击方系统崩溃。 4) WinNuke 攻击，主要是攻击目标端口，被攻击的目标端口一般是 139、

参数	说明
	138、137、113、53 等，WinNuke 现已发展到不仅可以攻击单个 IP，还可以连续攻击一个 IP 地址段，造成属于此地址段的的主机发生死机或蓝屏等异常情况。 5) TCP Scan，攻击者通过检测 TCP 服务预留的 1024 个端口，比如即时消息服务等,获知哪些端口是打开的。打开的端口暗示着安全漏洞，这些漏洞可以被恶意的黑客利用。 6) IP Option，攻击者通过检查 IP 包中的选项域，使用这个规则选项搜索 IP 包头的特定选项，例如源路由来指定路由，利用可信用户对服务器进行攻击。特别是基于 UDP 协议，由于是面向非连接的，更容易被利用来攻击。 7) Teardrop 利用了被攻击方对于 IP 碎片的重新组合来实施攻击，当服务器尝试重新组合含有错误分片信息的封包时会引起系统崩溃。 8) Targa3 是一种整合了多种拒绝服务攻击的工具包，可以通过多种方式对被攻击对象发动拒绝服务攻击。
统计型攻击	选择安全网关可以防御的统计型攻击防护类型，包括：SynFlood、UdpFlood、IcmpFlood、IpSweep 和 PortScan。网络卫士安全网关只检测已选择的攻击类型。 说明： 1) SYN Flood 是当前比较流行的拒绝服务攻击的方式之一。SYN Flood 利用了 TCP 协议的固有缺陷，通过发送大量伪造的 TCP 连接请求，使被攻击方充满了 SYN 半连接，从而耗尽被攻击方的资源而无法响应正常请求。 2) UDP Flood 是当前比较流行的拒绝服务攻击的方式之一。攻击者通过发送大量的含有 UDP 数据报的 IP 封包，以至于受害者再也无法处理有效的连接时，就发生了 UDP 泛滥。 3) ICMP Flood 通过向被攻击者发送大量的 ICMP 回应请求，消耗被攻击者的资源来进行响应，直至被攻击者再也无法处理有效的网络信息流时，就发生了 ICMP 泛滥。 4) IP Sweep (IP 扫描) 是一种简单的网络地址扫描方式，通过发送 ICMP 回应请求到某一地址段的所有主机，根据响应情况分析被扫描网络及主机的基本情况。IP Sweep 一般来说是恶意攻击的第一步。 5) Port Scan (端口扫描)，通过向一个特定主机地址的不同端口 (包括 TCP 端口和 UDP 端口) 发送 IP 数据包，以确定该主机开启的服务。

b) 点击“确定”完成 IDS 规则设置。

3) 修改 IDS 规则。

点击规则对应的“修改”图标，可以在弹出的修改窗口中修改规则。

4) 删除 IDS 规则

点击规则对应的“删除”图标可以删除规则。

14.3.2 黑白名单设置

为了提高 IDS 统计类攻击类型的检测效率，IDS 模块实现了黑白名单功能。通过在会话中统计某 IP 的有效连接个数，可以将该地址加入白名单；当 IDS 模块检测到 flood 攻

击或者调用 IDS 接口的其他模块判断某个地址是攻击源的时候，可以将该地址加入黑名单。IDS 模块将会直接丢弃黑名单上的 IP 报文，并直接放行白名单上的 IP 报文。

配置攻击防护的具体操作步骤如下所示：

1) 选择 **入侵防御 > Anti-DOS**，并激活“黑白名单”页签，如下图所示。

IDS规则	黑白名单	攻击统计
攻击防护类型		
Flood攻击加入黑名单 ☐ 启用 白名单 ☒ 启用 TCP首包可信检测 ☐ 启用 成为可信连接的最小报文数 5 [0-65535] 加入白名单的最小可信连接数 10 [1-65535] 黑/白名单超时时间 30 [1-60分钟]		
应用		

2) 设置有关攻击防护的参数，参数说明如下表所示。

参数	说明
Flood 攻击是否加入黑名单	选择是否开启统计型攻击的黑名单功能。 可选值：是、否。
白名单	选择是否开启白名单功能。 可选值：开、关。
TCP 首包可信检测	选择是否开启 TCP 首包可信检测功能。开启该功能后，要求经过网络卫士安全网关的 TCP 连接的首报文必须是 SYN 报文，非 SYN 报文的 TCP 首包将被丢弃。 可选值：是、否。 说明： 当网络卫士安全网关初次加入某个网络时，如果开启了 TCP 首包可信检测功能，则网络中原有 TCP 连接的非首包在经过刚加入的安全网关时均被丢弃，导致 TCP 连接中断，所以管理员需要根据实际网络环境决定是否开启 TCP 首包可信检测功能。
成为可信连接的最小报文数	设置成为可信连接的最小报文数，即只有当一个连接的双向报文数达到某个阈值时，该连接才能成为可信连接。 取值范围：0-65535。 说明： 此参数仅当白名单功能开启时出现。
加入白名单的最小可信连接数	设置加入白名单的地址的最小可信连接数，即只有当某个地址的可信连接达到某个阈值时，该地址才能被加入到白名单中。 取值范围：1-65535。 说明： 此参数仅当白名单功能开启时出现。
黑/白名单超时时间	设置黑/白名单的超时时间，即当一个地址被加入到黑/白名单后，经过一段时间，会将其从黑/白名单中删掉，其状态被置为初始状态。 单位：分钟；取值范围：1-60 分钟。

参数设置完成后，点击“应用”按钮即可。

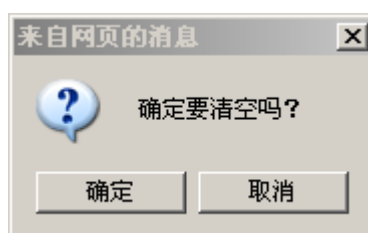
14.3.3 攻击统计显示

管理员可以查看攻击统计信息。

1) 选择 **入侵防御 > Anti-DOS**，并激活“攻击统计”页签，可以显示所有类型攻击次数的统计信息，如下图所示。

IDS规则 黑白名单 攻击统计						
统计清零						
ipoption	tcpscan	winnuke	icmptdrt	smurf	land	pingofdeath
0	0	0	0	0	0	0
targa3	ipspooft	portscan	synflood	udpflood	icmpflood	ipsweep
0	0	0	0	0	0	0
总计: 0 统计开始时间: +00 2010-04-26 08:37:24						

2) 点击“统计清零”，在弹出的如下图所示对话框中点击“确定”按钮，可以将各种统计信息清零。



14.4 防 ARP 欺骗

ARP 防欺骗功能主要防止局域网内的某些计算机冒充网关设备的 IP 地址发送 ARP 信息，导致正常计算机无法访问设备或外网的情况。启用该功能后，管理员还可以选择是否让网关设备定期发送其自己的 ARP 信息（主动发送免费 ARP 报文），以更新局域网中计算机设备上与网络卫士安全网关相关的 ARP 信息。

防 ARP 欺骗的设置步骤为：

1) 选择 **入侵防御 > 防ARP欺骗**，界面如下图所示。

防ARP欺骗		
+ 添加		总计: 0
接口名称	免费ARP发送间隔(/秒)	操作

2) 点击“添加”，设置规则，界面如下图所示。



防ARP欺骗配置界面。包含以下元素：

- 标题：防ARP欺骗
- 接口名称：eth0 (下拉菜单)
- 免费ARP发送间隔：1 [1-1800秒] (输入框)
- 底部按钮：确定、取消

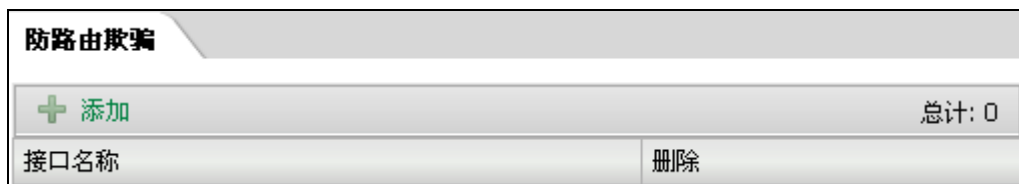
设定发送免费 ARP 报文的接口，以及发送时间间隔，点击“确定”按钮完成设置。

14.5 防路由欺骗

在网络卫士安全网关上可以开启接口路由的反向路径查询功能，这个功能检查指定接口接收的每一个经过设备的数据包。在设备的快速路径转发表中，该数据包所到达网络接口的所有路由项中，如果没有该数据包源 IP 地址的路由，路由器将丢弃该数据包。通过反向路径查询，可以有效防止基于源地址欺骗的网络攻击行为。

防路由欺骗的设置步骤为：

1) 选择 入侵防御 > 防路由欺骗，界面如下图所示。



防路由欺骗主界面。包含以下元素：

- 标题：防路由欺骗
- 操作按钮：+ 添加 (绿色)
- 统计信息：总计: 0
- 列表表头：接口名称、删除

2) 点击“添加”，增加规则，界面如下图所示。



防路由欺骗-开启反向路径查询配置界面。包含以下元素：

- 标题：防路由欺骗
- 子标题：开启反向路径查询
- 接口名称：eth0 (下拉菜单)
- 底部按钮：确定、取消

选择接收报文的接口，点击“确定”按钮启动接口的反向路径查询功能。

14.6 IDS 联动

一个安全系统较难实现所有的安全技术，IDS、反病毒、内容审计等都包括在网络卫士安全网关中会带来管理维护的巨大压力，也会降低网络卫士安全网关的性能，这对于处于网关角色的网络卫士安全网关来说是不合适的。首先，IDS 需要经常性地升级攻击模式库，而对网络卫士安全网关这样在关键部位工作的设备进行经常升级显然是不合适的。其次，如果网络卫士安全网关所包含的额外功能过多，自然会降低其运行速度，给内部网络和外部网络的通信造成瓶颈。

网络卫士安全网关充分考虑了用户使用和安全系统构建的方便性和易维护性，可以与主流的 IDS 和反病毒厂家的产品进行联动（网络卫士安全网关可以接受其他设备的联动请求，但并不主动探测）。

设置 IDS 联动的具体操作步骤如下所示：

1) 点击 **入侵防御 > IDS联动**，右侧页面如下图所示。

IDS联动

IDS联动配置

设置

+

添加

清空

总计: 0

ID	设备地址	共享密钥	操作

联动状态

刷新

清空

总计: 0

ID	控制	源MAC	目的MAC	源IP	目的IP	协议	源端口	目的端口	存活时间(秒)	操作

2) 配置 IDS 联动日志开关。

a) 点击“设置”按钮，配置是否记录 IDS 联动日志，界面如下图所示。

IDS联动日志

增加联动规则时记录日志

关

报文被阻止时记录日志

关

应用

参数说明见下表所示。

参数	说明
增加联动规则时记录日志	选择是否在增加联动规则时记录日志。 可选值：开、关。

报文被阻止时记录日志	选择是否在报文被阻止时记录日志。 可选值：开、关。

b) 设置完成后，点击“应用”按钮即可。

启动IDS联动日志后，根据 **日志与报警 > 日志设置** 中的配置，可以将相应的日志记录到本地或日志服务器中，具体操作请参见 [17.1日志设置](#)。

3) 配置安全网关的地址和可以联动的 IDS 设备的 IP 地址。

a) 点击“IDS 联动配置”右侧的“添加”，进入配置界面，如下图所示。



IDS联动配置

防火墙地址

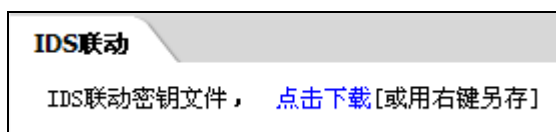
IDS地址

确定 取消

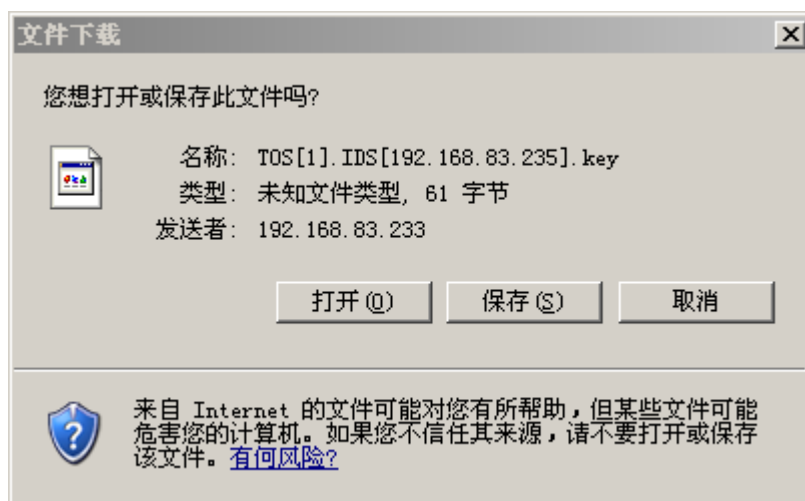
界面参数说明见下表所示。

参数	说明
安全网关地址	设置与 IDS 设备联动的安全网关接口的地址。 说明： 不能与进行联动的 IDS 设备配置相同的 IP 地址。
IDS 地址	设置联动安全网关的 IDS 设备的地址。 说明： 不能与进行联动的安全网关配置相同的 IP 地址。

b) 参数设置完成后，点击“确定”按钮，系统将自动生成 IDS Key 文件，并提示下载，如下图所示。



c) 点击“点击下载”蓝色链接，系统将提示是否打开或保存文件，如下图所示。



d) 点击“保存”按钮，然后选择文件的保存路径将文件保存到指定路径。默认的保存文件名为“TOS[1].IDS[192.168.83.235].key”，文件名中标出了与安全网关联动的 IDS 设备的 IP 地址信息。

使用文本工具查看该文件的内容，可以看到如下的信息。



此时，IDS 设备已添加到 IDS 联动列表中，与联动 IDS 设备共享的密钥也显示在列表中，如下图所示。

IDS联动			
IDS联动配置			
设置 + 添加 清空			总计: 1
ID	设备地址	共享密钥	操作
8328	192.168.83.235	1819A2CC259049CE	

e) 点击待删除联动条目右侧的“删除”图标，可以删除该联动信息。

f) 点击 IDS 联动列表右上方的“清空”，可以批量删除所有的联动信息。

4) 管理联动后的动态 PF 规则。

- a) 点击“联动状态”右侧的“刷新”，可以实时显示与 IDS 设备联动后得到的所有动态的 PF 规则。
- b) 点击待删除动态 PF 规则条目右侧的“删除”图标，可以删除该动态 PF 规则。
- c) 点击“联动状态”右侧的“清空”，可以清空与 IDS 设备联动后得到的所有动态的 PF 规则。

15 反垃圾邮件

网络卫士安全网关支持对 SMTP 协议的反垃圾邮件功能。

管理员通过配置邮件地址和 IP 地址黑白名单，对于通过 SMTP 协议传输的邮件进行过滤。还可以通过连接第三方的 DNS 服务器查找实时黑名单，过滤垃圾邮件。

需要注意的是，只有内容安全策略对象中开启了反垃圾邮件过滤功能，并且在访问控制规则中引用该内容安全策略对象，反垃圾邮件功能才会生效。否则即使此处设置了策略，也不会生效。访问控制规则设置请参见 [9.2.5添加规则](#)。内容安全策略设置请参见 [9.6内容安全策略](#)。

本章内容包括：

- 黑白名单。介绍如何设置邮件发件人 IP 地址以及邮件地址的黑白名单，来实现对垃圾邮件的过滤功能。
- 实时黑名单：介绍如何配置实时邮件黑名单服务以对抗垃圾邮件的泛滥。
- 灰名单技术：介绍如何通过灰名单技术对垃圾邮件进行过滤。
- 统计信息：介绍如何查看反垃圾邮件各个模块拦截到的垃圾邮件个数的统计信息。

15.1 黑白名单

在内容安全策略中启动 SMTP 协议的反垃圾邮件过滤功能后，安全网关设备使用 IP 地址黑白名单与邮件地址黑白名单来过滤经过设备传输的邮件。

反垃圾邮件检查是通过检查其发件人的邮件地址及 IP 地址是否匹配黑白名单，来确认邮件是否为垃圾邮件。匹配黑白名单的顺序是 ① “IP 地址白名单” ② “邮件地址白名单” ③ “IP 地址黑名单” ④ “邮件地址黑名单”。如果黑白名单均不匹配，则直接放行数据去进行后续检查。

对以 SMTP 协议发送的邮件，如果命中白名单，则此处放行；如果命中黑名单，邮件将被拦截，同时发件人会收到邮件被拦截的提示信息（512 网关提示）。

15.1.1 设置邮件地址黑白名单

“白名单”优先级高于“黑名单”，当一个邮件地址同时存在于邮件地址黑名单和邮件地址白名单时，白名单优先级较高，则邮件不会被作为垃圾邮件处理，直接放行。

邮件地址黑白名单设置方法为：

1) 在左侧导航菜单中选择 **反垃圾邮件 > 黑白名单**，并激活“邮件地址黑白名单”页签，界面如下图所示。系统默认不开启邮件地址黑白名单过滤功能。

邮件地址黑白名单 **IP地址黑白名单**

邮件黑名单设置

邮件地址黑名单

<-

X

邮件白名单设置

邮件地址白名单

<-

X

(注释：邮件黑白名单支持通配符，必须含有@符号。
例如：*Tom@spam.com*)

应用 清空配置

参数说明如下表所示：

参数	说明
邮件地址黑名单	在右侧的文本框中输入邮件地址格式的字符串，点击“<-”添加到左侧列表中。 说明： 支持通配符“*”和“？”，格式为“lisi@topsec.com.cn”。长度小于 63 个字节，最多可设置 64 个。
邮件地址白名单	在右侧的文本框中输入邮件地址格式的字符串，点击“<-”添加到左侧列表中。 说明： 支持通配符“*”和“？”，格式为“lisi@topsec.com.cn”。长度小于 63 个字节，最多可设置 64 个。

2) 参数值设置完成后，点击“应用”按钮，完成设置。

3) 点击“清空配置”按钮，系统弹出如下图所示的确认对话框。



点击“确定”后系统再次弹出如下图所示对话框，



再次点击“确认”，将删除所有已输入参数。

15.1.2 设置 IP 地址黑白名单

“白名单”优先级高于“黑名单”，当一个邮件的 IP 地址同时存在于 IP 地址黑名单和 IP 地址白名单时，白名单优先级较高，则邮件不会被作为垃圾邮件处理，直接放行。

IP 地址黑白名单设置方法为：

1) 在左侧导航菜单中选择 **反垃圾邮件 > 黑白名单**，并激活“IP地址黑白名单”页签，界面如下图所示。系统默认不开启IP地址黑白名单过滤功能。

参数说明如下表所示：

参数	说明
IP 地址黑名单	在右侧的文本框中输入 IP 地址格式的字符串，点击 “<-” 添加到左侧列表中。 说明： 不支持通配符，最多可设置 64 个。
IP 地址白名单	在右侧的文本框中输入 IP 地址格式的字符串，点击 “<-” 添加到左侧列表中。 说明： 不支持通配符，最多可设置 64 个。

2) 参数值设置完成后，点击“应用”按钮，完成设置。

3) 点击“清空配置”按钮，系统弹出如下图所示的确认对话框。



点击“确定”后系统再次弹出如下图所示对话框，



再次点击“确定”，将删除所有已输入参数。

15.2 实时黑名单

对于 SMTP 协议，网络卫士安全网关提供根据实时黑名单（RBL）查询服务来预防垃圾邮件通过安全网关进行传输。管理员首先要配置黑名单服务器的域名，当安全网关收到发送邮件的数据包时，会向黑名单服务器发送 DNS 查询请求，以确认发件服务器的 IP 地址是否在 RBL 中，如果在，则根据内容安全策略中的设置，拒绝其发送邮件的请求或者记录相关情况。

相关配置有：

（1）安全网关通过向黑名单服务器发送DNS查询请求，因此需要保证安全网关能够连接到Internet；还需要设置好DNS服务器，DNS服务器具体参数设置请参见 [6.9域名解析](#)。

（2）要使用实时黑名单进行反垃圾邮件过滤，需要管理员在定义内容安全策略对象时启用“实时黑名单”（请参见 [9.6内容安全策略](#)），并且在ACL策略中引用该内容安全策略对象（请参见 [9.2.5添加规则](#)）。那么，当数据报文匹配ACL规则时，将使用实时黑名单进行查询服务。

配置实时黑名单的步骤为：

1) 选择 **反垃圾邮件** > **实时黑名单**，界面如下图所示。

实时黑名单		
+ 添加 重置 清空		
提供商	RBL域名后缀	操作
cbl	cbl.anti-span.org.cn	 
xbl	xbl.spambaus.org	 

列表中显示出厂配置中系统内置的 RBL 服务器的信息，默认为“启用”状态，点击“状态”一栏的图标可以启用或禁用该 RBL 服务器。

2) 添加 RBL 服务器

a) 点击“添加”按钮，界面如下图。

参数说明如下表所示：

参数	说明
提供商	输入 RBL 服务器提供商的名称。
RBL 域名后缀	输入 RBL 服务器的 URL 地址。
启用实时黑名单	勾选即可启用，只有启用后才会向该服务器发送查询信息。 说明： 也可以添加后勾选“启用”一栏的复选框进行启用。

点击“确定”按钮完成添加。

3) 删除 RBL 服务器

点击“删除”一栏对应的图标可以删除该服务器。点击“清空”按钮，可以一次性删除所有的 RBL 服务器。

4) 恢复出厂配置

点击“重置”按钮，系统将恢复出厂配置中系统内置的 RBL 服务器配置。

15.3 灰名单技术

网络卫士安全网关支持启用灰名单技术进行反垃圾邮件。

其工作原理是：

灰名单技术基于一种重试的原则，即第一次看到某个 IP 要想给某个收件人发信，那么它将简单的返回一个临时错误，并拒绝此请求，但是在系统中记录发送邮件的 IP 地址和发件人信息。正常的邮件服务器都会在一段时间内重发一次邮件，如果重发邮件的时间间隔在系统设定的时间内，而且和系统记录的发件人的 IP 地址和邮件地址向匹配，则系统将此 IP 地址和邮件地址加入可信任列表，并对邮件予以放行。如果是非正常的邮件，那么或者将永远也不再进行重试，或者会疯狂重试，但由于间隔太近，而遭拒绝。因此，只要在灰名单的参数中设置一个合适的放行间隔，就可以在很大程度上对这类垃圾邮件有着良好的免疫能力。灰名单的一大特点就是不会丢失邮件，但是最大缺点是延迟（delay），为了避免影响用户正常发送邮件，可以设置工作时间内不进行灰名单检测。

设置灰名单相关参数的步骤描述如下：

1) 选择 **反垃圾邮件** > **灰名单技术**，界面如下图所示。

灰名单	
灰名单	
对不信任的发件人初始延迟时间	4 [1-59分钟]
在多长时间内在重复发送的邮件将被允许	31 [1-60小时]
保存被信任的发件人信息时间	36 [36-60天]
在工作时间时自动关闭灰名单功能	☐
工作时间	00:00 到 00:00
确定 清除设置	

参数说明如下表所示：

参数	说明
对不信任的发件人初始延迟时间	设置邮件最小重发间隔时间，单位：分钟。（默认值为 4）。
在多长时间内在重复发送的邮件将被允许	等待邮件重发最长时间，范围为 1-60，单位：小时。（默认值为 25）。
保存被信任的发件人信息时间	设置灰名单（包括可信任列表和不可信任列表）在系统中的保留时间，超过设定的时间后，将从系统中删除灰名单信息。范围为 36-60，单位为天。默认值为 36。
在工作时自动关闭灰名单功能	设置是否在“工作时间”设置的时间段内自动关闭灰名单检测功能，如果勾选，则只有在非工作时间内启动灰名单检测功能。
工作时间	设定工作时间的开始和结束时刻。

点击“确定”完成参数设置。点击“清除设置”，可以将界面设置的参数恢复出厂配置。

15.4 反垃圾统计

网络卫士安全网关提供了反垃圾邮件的统计功能，通过该功能可以查看 IP 白名单、IP 黑名单、邮件白名单、邮件黑名单、灰名单、反向 DNS 查询、实时黑名单等的命中次数。

具体的查看方法为：

选择 **反垃圾邮件** > **反垃圾统计** 进入统计页面，如下图所示。

统计信息							
统计清零							
统计开始时间	IP白名单	IP黑名单	邮件白名单	邮件黑名单	灰名单	反向DNS查询	实时黑名单
2010-06-23/04:57:56	0	0	0	0	0	0	0

需要说明的是，当设备重启后，会重新开始统计，之前的统计数据会被清空。

16 高可用性

本章主要介绍了网络卫士安全网关的一些高级特性，主要包括：

- 接口联动。介绍当安全网关工作在流量负载均衡模式时，如何确保负责转发数据的安全网关的出接口和入接口的状态改变保持一致。
- 双机热备。介绍如何使用和实现网络卫士安全网关的双机热备功能。
- 链路备份。介绍如何设置网络卫士安全网关的链路备份功能。
- 服务器负载均衡。主要介绍了如何定义负载均衡服务器、负载均衡组，以及如何利用负载均衡满足用户的访问需求。

16.1 接口联动

接口联动主要用于安全网关工作在连接保护模式时，可以在短时间内根据单一接口的状态调整组内所有接口的状态，保证转发设备出接口和入接口状态的一致性。例如：当连接保护模式下的设备 A 负责转发数据的出口 down 掉时，属于同联动组的入口状态也同步 down，则入口所连设备将会判断入口 down 了，就可以及时将数据通过其它的设备 B 进行传输。

接口联动组的配置和接口联动功能的启用步骤如下所示：

- 1) 点击导航树菜单 **高可用性 > 接口联动**，界面如下图。



- 2) 添加联动组

接口联动组的配置必须在接口联动功能处于“停止”状态时进行，否则无法操作成功。

- a) 点击“添加”，如下图所示。

接口联动组属性

名称 *

可用接口

eth0
eth1
eth2
eth3

->

×

成员

确定
取消

界面参数说明如下表所示。

参数	说明
名称	输入接口联动组的名称。 最多不能超过 31 个字节。
成员列表	选择接口联动组中的接口成员。 “选择成员”下的文本框中列出了设备当前所有的物理接口，选中该文本框中的接口后，点击“→”按钮将其添加到联动组中；“已经选择”下的文本框中列出了联动组中当前包括的接口，选中该文本框中的接口后，点击“×”按钮将其从联动组中删除掉。 说明： 1) 联动组的接口成员可以是安全网关的物理接口或链路聚合口，不支持子接口和 VLAN； 2) 同一个物理接口不能同时属于不同的联动组，并且每个联动组的成员数不能低于两个，不能高于八个。 3) 已经加入到链路聚合中的接口不能再加入到接口联动组中。

b) 参数设置完成后，点击“确定”按钮，完成接口联动组的添加。此时，接口联动组处于“未运行”状态，如下图所示。

接口联动

联动功能 启用 停止

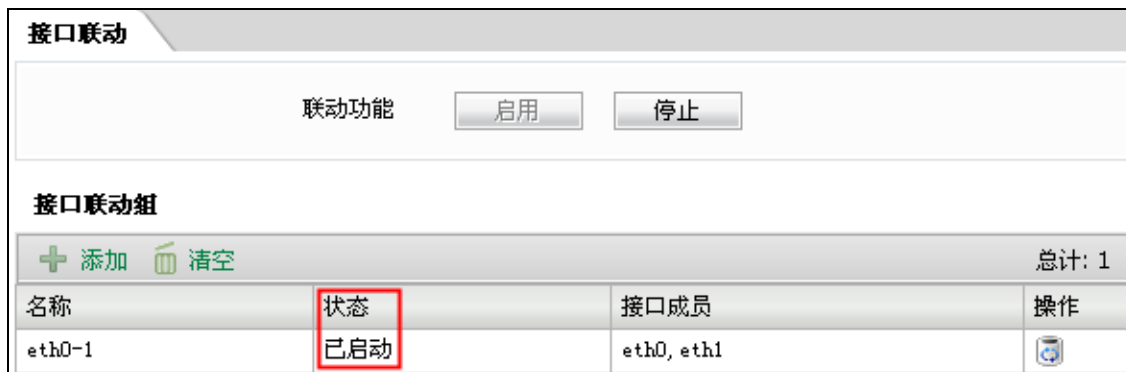
接口联动组

+ 添加 清空
总计: 1

名称	状态	接口成员	操作
eth0-1	未运行	eth0, eth1	🔄

3) 启动接口联动功能

勾选“联动功能”右侧的“启用”，启动接口联动功能。此时，接口联动组处于“已启动”状态，如下图所示。



此后，当该联动组内的一个物理接口 down 后，该组内所有的物理接口都同步 down 掉。

4) 删除联动组

删除某个联动组时，必须先停止接口联动功能，然后点击待删除联动组条目后的“删除”图标进行删除。

点击“清空”，可以一次性删除所有的联动组。

16.2 高可用性

在数据通信过程中，各种软件或硬件错误都可能导致网络连接异常中断，造成数据传输失败。为了避免网络设备或线路出现故障时引起数据通信中断，网络卫士安全网关提供了双机热备功能，以确保在通信线路或设备故障时提供备用方案，有效增强网络的可靠性。

目前，网络卫士安全网关可以实现多种方式下的冗余备份，包括：双机热备模式、负载均衡模式和连接保护模式。双机热备模式和负载均衡模式下，需要通过 VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）完成安全网关主备状态的协商；连接保护模式下，由上下游设备决定流量的走向，安全网关之间只做连接同步，并不建立主备状态。下面分别对这三种模式的配置进行详细介绍。

说明

- ✧ 安全网关在做双机热备时，必须使用心跳口交换状态监测及探测信息，网络卫士安全网关上的任何以太网接口都可以做为心跳接口，但对于有专门心跳口的设备，建议使用心跳口。
- ✧ 安全网关的接口均为自适应接口，心跳口之间的连线既可以使用交叉线也可以使用直连线。
- ✧ 安全网关双机热备功能的三种模式均最多支持 8 台安全网关。
- ✧ 如果访问控制规则中引用了 AV 或内容安全策略，则无法保证匹配此条规则的应用流量在主备切换前后能够维持。

16.2.1 双机热备模式

在双机热备模式下，任何时刻都只有一台安全网关（主设备）处于工作状态，承担报文转发任务，一组安全网关处于备份状态并随时接替任务。当主设备的任何一个接口（不包括心跳口）出现故障时，处于备份状态的安全网关（从设备）经过协商后，由优先级高的安全网关接替主设备的工作，进行数据转发。

多台网络卫士安全网关之间各通过一个物理接口（心跳口）相连，用于多台安全网关之间的状态和配置信息的同步。

网络卫士安全网关双机热备模式的部署示意图如下所示（最多支持 8 台设备）。

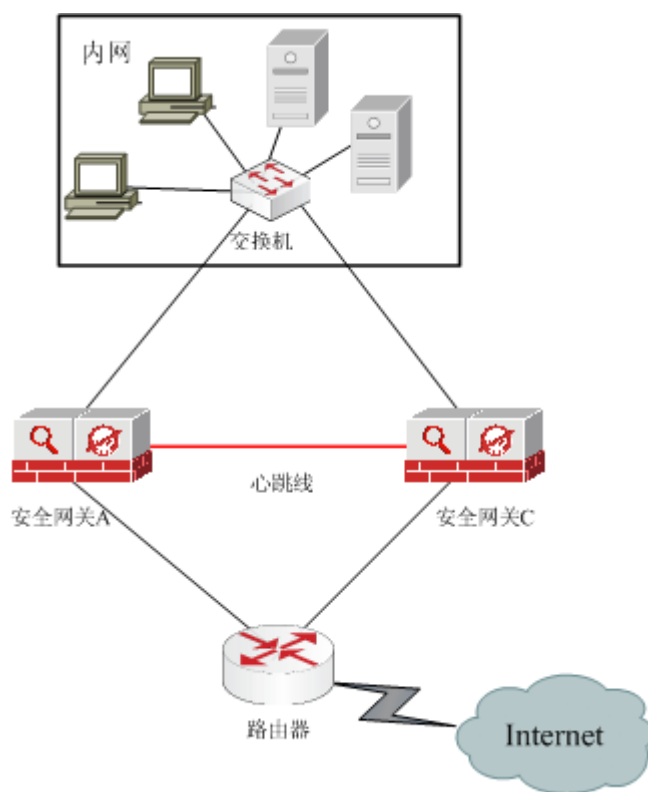


图 16-1 网络卫士安全网关双机热备模式示意图

在双机热备模式部署时，管理员必须在主从设备上首先对接口进行相关配置（具体请参见 [6.2.1物理接口](#)）：

① 配置心跳口属性。

要求：所有心跳口的地址必须配置在同一网段，而且接口属性必须要勾选“非同步地址”选项，否则心跳口的 IP 地址信息会在主从设备运行状态同步时被对方覆盖。

② 配置除了心跳口以外的其他通信接口的属性

要求：互为备份的接口必须配置相同的 IP 地址。

之后，再配置双机热备的相关参数，并启用双机热备功能。

步骤如下：

1) 点击 **高可用性 > 高可用性**，在“HA模式”处选择“双机热备”，如下图所示。

高可用性配置

HA 模式 双机热备

心跳地址 本地 *
 对端 *

热备组	热备组	本地/对端	身份	抢占	工作状态
100 *	本地	主	开启		

监控接口 eth0 增加

启用
停止
应用

同步操作

对端机同步到本机
本机同步到对端机

切换操作

备份组主动状态切换

2) 设置双机热备参数，参数说明如下表所示。

参数	说明
心跳地址：本地	配置本机上作为心跳口的物理接口的 IP 地址。
心跳地址：对端	设置对端设备心跳口的 IP 地址，或本地地址所在子网的子网广播地址。 说明： （1）对端地址和本地地址必须在同一子网内，而且必须勾选“非同步地址”选项，否则无法配置成功； （2）只有两台设备进行双机热备时，建议将“对端地址”设为单播地址；超过两台设备时，必须将“对端地址”设为本地地址所在子网的子网广播地址（最多支持八台对端设备）。
热备组	设置除心跳口以外的通信接口所属的 VRRP 备份组的组号，网络卫士安全网关将根据组号映射生成相应的 VRRP 组的虚拟 MAC 地址。默认为 100，取值范围：1-255。 说明： 一般情况下需要管理员不需要修改该值。如果实际网络中出现 VRID 相同的两台设备连接在同一个交换机上的情况，需要修改该值以防止 VRID 配置冲突。

参数	说明
身份	选择该安全网关的身份：主或从。
抢占	设置是否开启“抢占”模式，即主网关宕机后，之后重新恢复正常工作时，是否重新夺回主网关的地位。 说明： 只有当主网关与从网关相比有明显的性能差异时，才需要配置主网关工作在“抢占”模式，否则当主网关恢复工作时主从网关的再次切换浪费系统资源，没有必要。
监控接口	将接口设置为“监控接口”指的是将通信接口加入“热备组”设置的 VRID 组，并设置该接口的 HA 权重值。 说明： 1. 如果要想实现接口的双机热备，则必须分别选择所有通信接口，点击“增加”按钮将其加入 VRID 组，并且启用“监控”功能。 2. HA 权重：一般情况下，由设备的“身份”决定其工作状态为主设备或从设备。当由于某种原因（例如互为备份的接口同时 down 掉）使得互为备份的接口优先级相同时，则由此处设置的“HA 权重值”来决定 vrid 组的工作状态。HA 权重值的范围为：1-100。

b) 参数设置完成后点击“应用”按钮，保存配置。

3) 启动双机热备模式

界面参数设置完成后，点击“启用”按钮，启动双机热备模式，如下图所示。

高可用性配置

HA 模式 双机热备

心跳地址 本地 172.16.1.1 *
 对端 172.16.1.2 *

热备组	热备组[1-255]	身份	抢占	HA 权重	HA 权重[0-100]	工作状态
	100 *	主	开启			工作机

监控接口 eth0 增加

接口名称	接口监控	HA 权重[0-100]
eth0	☒	0

启用
停止
应用

“工作状态”一栏显示了当前设备的身份为“工作”或“备份”。

4) 手工同步配置

当主网关或从网关配置发生变更后，手工同步配置可以保证主从网关配置的一致性。



点击“对端机同步到本机”按钮，可以从对端机同步配置到本机，包括除 HA 之外的所有配置信息。

点击“本机同步到对端机”按钮，可以从本机同步配置到对端机上，包括除 HA 之外的所有配置信息。

5) 手工切换主备机状态

根据实际情况需要，可以手工切换备份组主机和备机的状态。



点击“备份组主动状态切换”按钮，可以互换主机和备机的状态。

6) 停止双机热备模式

点击“停止”按钮，可以停止双机热备模式。

16.2.2 负载均衡模式

在负载均衡模式下，两台/多台安全网关并行工作，都处于正常的数据转发状态。每台安全网关中设置多个 VRRP 备份组，两台/多台安全网关中 VRID 相同的组之间可以相互备份，在某个 VRID 组中，优先级较高的安全网关在该 VRID 组中为主设备；当优先级相同但不为 0 时，根据安全网关启动 HA 的顺序确定工作状态，最先启动 HA 的安全网关在该 VRID 组中为主设备；当优先级均为 0 时，根据每台安全网关上该 VRID 组的接口 HA 权重值来确定工作状态，值大的设备在该 VRID 组中为主设备。以便确保某台设备故障时，其他的设备能够接替其工作。

如安全网关 A 既可以作为备份组 1 的主设备，同时又兼任备份组 2 的从设备，而安全网关 B 恰好相反，可以作为备份组 1 的从设备，同时兼任备份组 2 的主设备。这样，一部分主机使用备份组 1 作为网关，另一部分主机使用备份组 2 作为网关，以达到分担数据流，而又相互备份的目的。

负载均衡模式部署示意图如下所示。

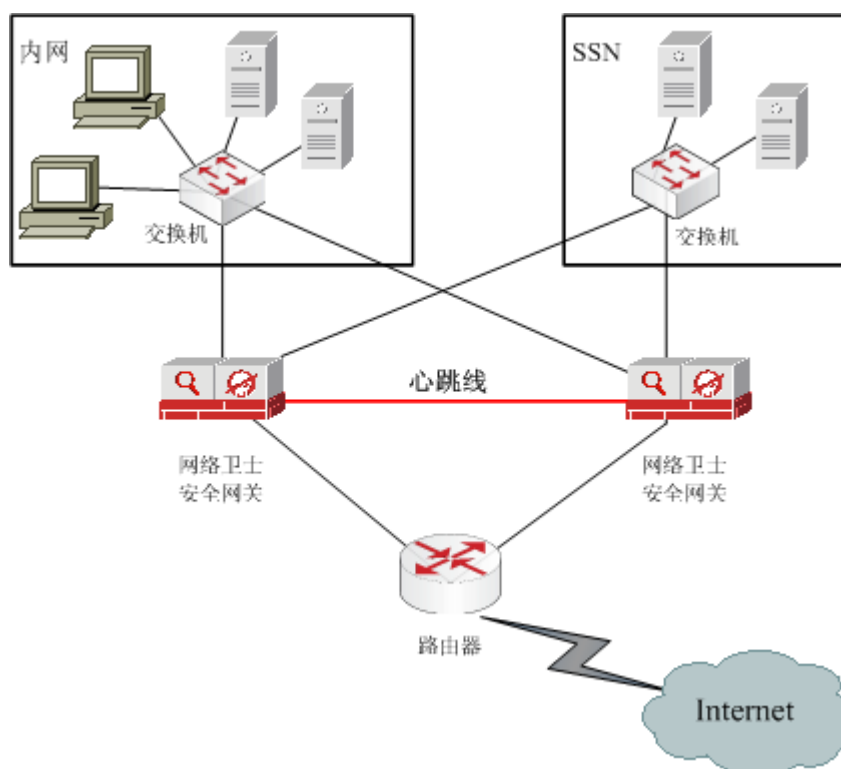


图 16-2 网络卫士安全网关负载均衡模式示意图

在负载均衡模式部署时，管理员必须在主从设备上首先对接口进行相关配置（具体请参见 [6.2.1物理接口](#)）：

① 配置心跳口属性。

要求：所有心跳口的地址必须配置在同一网段，而且接口属性必须要勾选“非同步地址”选项，否则心跳口的IP地址信息会在主从设备运行状态同步时被对方覆盖。

② 配置除了心跳口以外的其他通信接口的属性

要求：互为备份的接口必须配置相同的IP地址。

之后，再配置负载均衡相关参数，并启用负载均衡功能，具体包含如下配置：

（1）配置VRID组的属性。需要注意的是，在WEBUI界面中只能设置两个VRID组，如果VRID组需要配置多于两个时，需要在命令行下进行配置。（2）配置心跳口属性。（3）运行命令**#ha ip-probe add probeid <number>** 选择探测链路（*number*是链路探测的ID号，且必须是事先添加好的探测项，关于IP探测项的设置，请参见[6.8IP探测](#)）。

详细步骤如下：

1) 选择 **高可用性 > 高可用性**，然后在“HA模式”处选择“负载均衡”，如下图所示。

高可用性配置				
HA 模式	负载均衡			
心跳地址	本地		*	
	对端		*	
热备组		组ID	优先级	抢占
	组1			开启
	组2			开启
监控接口	eth0 增加			
启用 停止 应用				
同步操作				
对端机同步到本机 本机同步到对端机				

2) 设置负载均衡参数，参数说明如下表所示。

参数	说明
本地/对端地址	设置设备本机/对端设备心跳口的 IP 地址。 说明： (1) 对端地址和本地地址必须在同一子网内，否则无法配置成功； (2) 只有两台设备进行双机热备时，建议将“对端地址”设为单播地址；超过两台设备时，必须将“对端地址”设为本地地址所在子网的子网广播地址（最多支持八台对端设备）。
热备组	设置备份组的 ID 号和优先级，是否为抢占模式。 说明： (1) 备份组的 ID 号的取值范围为 1—255。 (2) “优先级”设置当前设备上该备份组的优先级。取值范围为 1—255。值越大，优先级越高；备份组中有接口宕掉后，该组优先级降为 0。 (3) “抢占”设置是否开启“抢占”模式，即主网关宕机后，之后重新恢复正常工作时，是否重新夺回主网关的地位。只有当主网关与从网关相比有明显的性能差异时，才需要配置主网关工作在“抢占”模式，否则当主网关恢复工作时主从网关的再次切换浪费系统资源，没有必要。 (4) “工作状态”显示当前该备份组的工作状态：显示为“工作”时，表示设备此时对该备份组而言是主设备；显示为“备份”时，表示设备此时对该备份组而言是从设备。

监控接口	将通信接口加入“热备组”设置的 VRID 组，并设置该接口的 HA 权重值。HA 权重值的范围为：1-100。 说明： 1. 如果要想实现接口的双机热备，则必须分别选择所有通信接口，点击“增加”按钮将其加入 VRID 组，选择该接口所属的 VRID 组。 2. HA 权重：一般情况下，由设备的“身份”决定其工作状态为主设备或从设备。当主备两台安全网关同时有属于相同 vrid 组的接口 down 掉时，则由 vrid 组的接口的 HA-metric 总值来决定 vrid 组的工作状态。通俗的讲，当主备安全网关都有接口 down 掉时，比较设备接口 HA-metric 的和，HA-metric 大的是主设备。 3. 监控接口可以是物理接口和虚拟接口。当 vlan 虚接口中有多个物理接口时，请尽量不要将 vlan 接口加入 vrid 组，而是将这个 vlan 下所有物理接口都加入 vrid 组。这样做的好处是，当主设备有一个物理接口 down 掉后，备用安全网关就会接管主设备的工作状态；如果只将 vlan 接口加入 vrid 组，只有在 vlan 所有接口都 down 掉时，备用安全网关才会接管主设备的工作状态。

b) 参数设置完成后点击“应用”按钮，保存配置。

3) 启用负载均衡模式

点击“启用”按钮完成配置，心跳口连接建立，“工作状态”一栏显示 HA 的当前状态。如下图所示。

高可用性配置

HA 模式 负载均衡

心跳地址 本地 *

对端 *

热备组	组ID[1-255]	优先级[1-255]	抢占	工作状态
	1 *	1 *	开启	工作
	2 *	4 *	开启	工作

监控接口 eth0 增加

接口名称	组1	组2	HA权重[0-100]
eth0	☐	☒	0

启用 停止 应用

4) 手工同步配置

当主网关或从网关配置发生变更后，手工同步配置可以保证主从网关配置的一致性。

点击“对端机同步到本机”按钮，可以从对端机同步配置到本机，包括除 HA 之外的所有配置信息。

点击“本机同步到对端机”按钮，可以从本机同步配置到对端机上，包括除 HA 之外的所有配置信息。

5) 停止负载均衡模式

点击“停止”按钮，可以停止负载均衡模式。

16.2.3 连接保护模式

在连接保护模式下，安全网关之间只同步连接信息，并不同步状态信息。当两台/多台安全网关均正常工作时，由上下游的设备通过运行 VRRP 或 HSRP 进行冗余备份，以便决定流量由哪台安全网关转发，所有安全网关处于负载分担状态，当其中一台发生故障时，上下游设备经过协商后会将其上的数据流通过其他安全网关转发。

连接保护模式下的部署示意图如下所示。

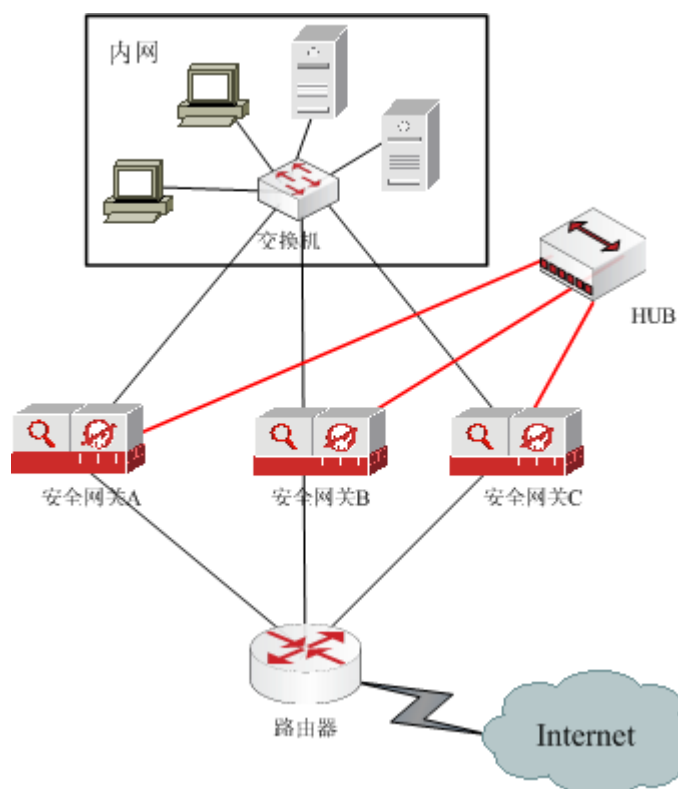


图 16-3 网络卫士安全网关连接保护模式示意图

网络卫士安全网关部署为连接保护模式时，管理员必须在主从设备上首先对接口进行相关配置（具体请参见 [6.2.1物理接口](#)）： 配置的步骤如下：

① 配置心跳口属性。

要求：所有心跳口的地址必须配置在同一网段，而且接口属性必须要勾选“非同步地址”选项，否则心跳口的 IP 地址信息会在主从设备运行状态同步时被对方覆盖。

② 配置除了心跳口以外的其他通信接口的属性

之后，再配置并启用连接保护模式。

1) 选择 **高可用性** > **高可用性**，然后在“HA模式”处选择“连接保护”前的单选按钮，如下图所示。

高可用性配置

HA 模式 ☒ 连接保护

心跳地址 本地 *

对端 *

同步操作

参数说明如下表所示。

参数	说明
本地心跳地址	设置本机心跳口的 IP 地址。 说明： 本地地址和对端地址必须在同一子网内，否则负载均衡功能无法配置成功。
对端心跳地址	设置对端设备心跳口的 IP 地址，或本地地址所在子网的子网广播地址。 说明： (1) 对端地址和本地地址必须在同一子网内，否则无法配置成功。 (2) 当两台设备进行负载均衡时，建议将“对端地址”设为单播地址；当超过两台的设备进行负载均衡时，必须将“对端地址”设为本地地址所在子网的子网广播地址（最多支持八台对端设备）。

2) 点击“应用”按钮可以保存配置。点击“启用”按钮，启动连接保护模式。

3) 手工同步配置

当主网关或从网关配置发生变更后，手工同步配置可以保证主从网关配置的一致性。

点击“对端机同步到本机”按钮，可以从对端机同步配置到本机，包括除 HA 之外的所有配置信息。

点击“本机同步到对端机”按钮，可以从本机同步配置到对端机上，包括除 HA 之外的所有配置信息。

4) 停止负载均衡模式

点击“停止”按钮，可以停止负载均衡模式。

16.3 链路备份

在网络设备的整个运行期间，无法保证设备所有接口都能长时间正常运作，或不可避免地会遇到一些可知或不可知因素造成设备某接口无法运行。网络卫士安全网关提供了“链路备份”功能来实时监视整个链路的工作情况，一旦发现异常，就立即启动“链路备份”功能自动切换到另一条备用链路，以确保网络的正常通信。

链路备份功能的设置步骤如下：

1) 选择 **高可用性 > 链路备份**，进入链路备份功能的设置页面，如下图所示。

链路备份			
链路类型	IP探测ID	状态	当前使用
主链路	-选择ID- *		
从链路	-选择ID- *		

参数说明如下表所示。

参数	说明
主链路	选择已经设置的IP探测链路ID，IP探测设置请参见 6.8IP探测 。
从链路	选择已经设置的 IP 探测链路 ID。 说明： 从链路和主链路不能选择同一个链路 ID。

2) 参数设置完成后，点击“设置参数”按钮，完成设置。

3) 设置默认静态路由

添加两条默认路由，设置其“探测ID”分别为此处设定的主从链路，并设置“出口”为IP探测模块设置的相应的链路接口。具体请参见 [6.4.1路由表](#)。

例如，设定主从链路分别为 ID 为 100 接口为 eth0 的链路，和 ID 为 101 接口为 eth1 的链路，则需要添加如下图所示的静态路由。

路由表

策略路由

动态路由OSPF

动态路由RIP

动态路由BGP

多播

标记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D-Dhcp, I-Ipsec, i-Interface specified

+ 添加

清空

总计: 10

目的	网关	标记	度量值	权重值	出接口(属性)	探测ID	删除
172.16.1.1/32	0.0.0.0	ULi	1	1	lo	-	-
12.12.12.1/32	0.0.0.0	ULi	1	1	lo	-	-
192.168.83.237/32	0.0.0.0	ULi	1	1	lo	-	-
172.16.1.0/24	0.0.0.0	UCi	10	1	eth1	-	-
12.12.12.0/24	0.0.0.0	UCi	200	1	sslvpn0	-	-
192.168.83.0/24	0.0.0.0	UCi	10	1	eth0	-	-
192.168.83.0/24	0.0.0.0	UCi	100	1	ipsec0	-	-
10.10.10.0/24	192.168.83.237	UGIi	100	1	ipsec0	-	-
0.0.0.0/0	192.168.83.1	UGSi	1	1	eth0	100	
0.0.0.0/0	172.16.1.2	UGSi	2	1	eth1	101	

4) 点击“启动”按钮，启动链路备份功能，如下图所示。

链路备份			
链路类型	IP探测ID	状态	当前使用
主链路	100 *	链路良好	*
从链路	101 *	链路良好	

启动
停止
设置参数
重置参数

启动链路备份功能时，会判断当前两条默认路由是否可用，如果不可用，就不启动，并且报错。

图中分别标出了主/从链路的状态，“链路良好”表示链路正常，“链路不可达”表示链路不正常。链路的状态是根据主/从链路与探测IP是否能通信来判断的。为了正常使用网络卫士安全网关的链路备份功能，需要保证主/从链路均为“链路良好”状态。“*”表示当前使用的链路。

16.4 服务器负载均衡

网络卫士安全网关可以根据用户需求和灵活的负载均衡算法，实现用户服务器的负载均衡，保证用户关键服务的有效性。网络卫士安全网关支持基于会话的负载均衡。

使用网络卫士安全网关的服务器负载均衡功能，可以通过以下三步来实现：

- 定义服务器

- 定义负载均衡组
- 定义地址转换规则

16.4.1 定义服务器

定义负载均衡组中的服务器，具体操作步骤如下：

- 1) 点击 **高可用性 > 服务器负载均衡**，然后选择“服务器”页签，如下图所示。



- 2) 点击页面中的“添加”，设置参与负载均衡的服务器，如下图所示。

服务器属性

名称 *

主机

权重 * [1-100]

探测选项

不作探测 ☒

主机探测 ☐

服务探测 ☐ 端口

参数说明如下表所示。

参数	说明
名称	负载均衡服务器名称。
主机	已定义的主机地址对象，表明该服务器的真实 IP 地址。 说明： 被服务器引用的主机对象中只能且必须包含一个 IP 地址。
权重	数值越大，当根据权重选择负载均衡方式时，该服务器承担的流量就越大。通常情况下根据服务器的性能或处理能力来定义权重，默认值为 1，取值范围为 1-100。
探测选项	可以是不做探测、主机探测和服务探测。 如果是服务探测还需要设置相应的端口号。主机探测是通过简单的 PING 命令进行定时监测，根据服务器是否在线来判断服务器状态；服务探测则是根据服务器提供的服务，选择相应的端口进行探测，如 HTTP 的 80 端口、FTP 的 20、21 端口或用户自定义的特殊端口。一般来说，服务探测更能精确地体现服务器是否可用。
端口	当选择为服务探测时，负载均衡服务器上提供该服务所使用的端口号。

说明

- ◇ 通过探测，可以检测服务器的工作状态，可以避免在该服务器宕机或服务异常的情况下仍旧发送流量到该服务器，造成用户请求的服务不能得到响应。

3) 参数设置完成后，点击“确定”按钮，完成设置负载均衡服务器的设置。

16.4.2 定义负载均衡组

负载均衡组的具体配置步骤如下：

1) 点击 **高可用性 > 服务器负载均衡**，然后选择“均衡组”页签，如下图所示。

服务器		均衡组			
		+ 添加 参数设置 清空 总计: 1			
ID	名称	成员	负载方式	备份服务器	操作

2) 点击页面中的“添加”，添加负载均衡组，如下图所示。

均衡服务器组属性

名称 *

可用服务器

负载均衡方式

☒ 轮流

☐ 根据权重轮流

☐ 最少连接

☐ 加权最少连接（最少连接算法再加上加权值）

☐ 根据源地址作HASH查找

☐ 根据目的地址作HASH查找

成员

备份组 -选择均衡组-

操作

确定
取消

参数说明如下表所示。

参数	说明

参数	说明
名称	设置服务器负载均衡组的名称。
选择服务器	选择要加入此均衡组的服务器。
负载均衡方式	设置对多个服务器进行负载分配时所依据的原则。 说明： 轮流：当负载均衡组中的所有服务器性能基本相同时，可以选择轮流选择的方式，网络请求会轮流分配给负载均衡组中的服务器。 根据权重轮流：根据服务器的权重值来分配服务请求流量。根据权重的负载均衡方式可以保证高性能的服务器负担较多的请求，性能差一点的服务器承担相对少一点的请求。 最少连接：记录服务器的当前连接数，将新连接分配到当前连接最少的服务器。 加权最少连接：在最少连接方式下根据系统定义的权值分配连接。 根据源地址作 HASH 查找：相同的源 IP 地址均衡到相同的服务器。 根据目的地址作 HASH 查找：相同的目的 IP 地址映射到相同的服务器上。
备份组	当本组中的所有服务器均停止服务时，负载均衡组中服务器的内容将备份到该处选择的负载均衡组。

参数设置完成后，点击“确定”按钮，完成负载均衡组的设置。

3) 点击页面中的“参数设置”，设置负载均衡组的基本参数，如下图所示。

负载均衡参数

服务器切换时间

* [0-30秒]

探测时间间隔

* [5-30秒]

探测的报文数

* [1-8个]

确定

取消

参数说明如下表所示。

参数	说明
服务器切换时间	设置两个均衡组之间服务器的切换时间。 取值范围为 0-30 秒。
探测时间间隔	设置本次探测与下一次探测之间的间隔时间。 取值范围为 5-30 秒。
探测的报文数	设置每次探测所发送的探测报文数目。 取值范围为 1-8 个。

参数设置完成后，点击“确定”按钮即可。

4) 在“均衡组”页面，点击待修改均衡组条目后的“修改”图标，可以修改均衡组信息。

5) 在“均衡组”页面，点击待删除均衡组条目后的删除图标，可以删除该均衡组信息。

正确定义了负载均衡组后，还需要设置相应的地址转换规则，这样才能将针对某一主机的访问请求通过负载均衡算法分配到负载均衡组中的各服务器。定义地址转换规则的操作步骤如下：

1) 选择 **防火墙 > 地址转换**，在右侧页面中点击“添加”，进入设置地址转换规则页面。具体参数含义请参见[9.4地址转换](#)。

2) 选择“目的转换”，并在“源”、“目的”和“服务”处分别选择需要转换的地址和服务。“目的”应设置为需要使用负载均衡组来分担网络负担的设备的 IP 地址，也就是向外部提供服务的虚拟 IP 地址。该地址可以通过添加主机对象来设置。

3) 在“目的地址转换为”项中设置转换后的目的地址为刚才已定义的负载均衡组。根据需要，也可以设置“目的端口转换”，实现对外提供服务的端口到真实服务端口的转化。通过“目的端口转换”，可以更好的隐藏内部服务器及网络结构。

4) 点击“确定”按钮，完成地址转换规则的设置。

至此，便彻底完成了负载均衡组的设置。

17 日志与报警

为了方便用户更好地调试、监控和管理网络卫士安全网关，网络卫士安全网关向用户提供了日志管理和报警功能。本章将逐一介绍，结构如下所示：

- 日志设置
- 日志查看
- 报警

17.1 日志设置

网络卫士安全网关提供完善的日志和报警服务功能，方便用户及时跟踪网络卫士安全网关的工作状态，并可结合天融信的网络卫士安全审计系统（TOPAudit），可以对网络中的各种设备和系统进行集中的、可视的综合审计分析，及时发现安全隐患，提高安全系统成效，并大大提高安全管理的方便性。

网络卫士安全网关可以按照 WELF 格式来记录日志，并通过 Syslog 协议传送到已设定的日志服务器上，并可以采用第三方软件来对日志进行统计与分析。

为网络卫士安全网关配置日志服务器的具体方法如下：

- 1) 点击导航菜单 **日志与报警** > **日志设置**，进入“日志设置”窗口，如下图所示。

日志设置

服务器地址

192.168.1.253

*[可输入多个IP地址，用空格分开]

服务器端口

514

*

传输类型

SysLog

是否传输

☒

是否加密

☐

日志级别

调试

日志类型

☐ 选择全部

☒ 配置管

☒ 系统运

☒ 阻断策

☒ 连接

☒ 理

☒ 行

☒ 略

☒ 用户

☒ 访问控

☒ 防攻击

☒ 深度内

☒ 认证

☒ 制

☒ 御

☒ 容检测

☒ 防病毒

☒ 端口流

☐ 入侵防

☒ 虚拟专

☒ 网

☒ 量

☒ 应用程

☒ 序识别

☒ 反垃圾

☒ 系统

☒ 全网接

☒ 应用

☒ 邮件

☒ 端口转

☒ 发

☒ WEB转发

SSLVPN日

☒ 系统

☒ 全网接

☒ 应用

志：

☒ 端口转

☒ 发

☒ WEB转发

应用

界面中各参数的含义如下表所示。

参数	说明
服务器地址	日志服务器的 IP 地址。
服务器端口	日志服务器开放的服务端口。
传输类型	使用的日志类型，可以是 Syslog 或 Welf。
是否传输	是否传输日志。
是否加密	日志信息传输时是否加密。
加密密码	日志信息传输时使用的加密密码。 说明： 加密密钥为 8 位。
日志级别	选择记录的日志级别，系统将会记录所选级别及其以上级别的日志信息。如选择严重，则系统将记录紧急、告警和严重级别的日志信息。 日志级别如下： 紧急——造成严重错误导致系统不可用，该日志被传送到日志服务器。 告警——警报信息，需要通知管理员，该日志被传送到日志服务器。 严重——严重错误信息，可能会造成某些功能无法正常工作。 错误——一般错误信息。 警示——所有攻击行为以及非授权访问（除通信日志外）。

参数	说明
	通知——管理员操作。 信息——普通事件。 调试——开发人员调试信息。
日志类型	选择希望记录的日志类型。 选中“日志类型”后的复选框后，再选择希望记录的日志类型。 日志类型包括：配置管理、系统运行、阻断策略、连接、访问控制、防攻击、深度内容检测、端口流量、用户认证、入侵防御、虚拟专网、防病毒、反垃圾邮件、应用程序识别、SSLVPN 日志（包括系统、全网接入、应用 web 化、端口转发和 WEB 转发）。

2) 设置日志服务器参数后，点击“应用”按钮即可完成日志设置。

说明

- ✧ 系统记录和传输日志是根据日志类型和日志级别。如日志级别为“严重”，日志类型为“阻断策略”，系统将记录紧急、告警和严重级别的阻断策略日志。
- ✧ 设置并应用日志服务器参数后，系统记录的日志除了被发送到设定的日志服务器中外，也在安全网关中缓存部分日志。在安全网关中缓存的日志可以通过 **日志与报警 > 日志查看** 进行查看，具体请参见 [17.2 日志查看](#)。

17.2 日志查看

管理员在“日志设置”模块设置并应用日志服务器参数后，系统记录的日志除了被发送到设定的日志服务器中外，也在安全网关中缓存部分日志。管理员可以查看在安全网关中缓存的日志信息，以及时跟踪网络卫士安全网关的工作状态。

17.2.1 常规日志

常规日志指的是安全网关系统运行期间有关系统运行状况、管理情况以及策略匹配情况等等的记录信息。

1. 查看日志

点击导航菜单 **日志与报警 > 日志查看**，并选择“常规日志”页签，进入“日志查询”窗口，如下图所示。

常规日志

深度内容过滤日志

病毒过滤日志

反垃圾邮件日志

应用程序识别日志

IPS日志

日志类型

系统运行

查找

查找

清空所有类型日志

刷新日志

总计: 4

日期/时间	级别	类型	描述
2009-11-19/14:49:46	告警	系统运行	id=tos fw=TopsecOS recorder=HA op=switch-master msg=" vrid[2] priority[4] ha-metric[0] preempt[enable]"
2009-11-19/14:49:46	告警	系统运行	id=tos fw=TopsecOS recorder=HA op=switch-master msg=" vrid[1] priority[1] ha-metric[0] preempt[enable]"
2009-11-19/14:49:45	告警	系统运行	id=tos fw=TopsecOS recorder=HA op=switch-master msg=" vrid[100] priority[254] ha-metric[0] preempt[enable]"
2009-11-19/14:39:12	告警	系统运行	id=tos fw=TopsecOS recorder=HA op=switch-master msg=" vrid[100] priority[254] ha-metric[0] preempt[enable]"

界面中默认显示系统中所有缓存的“系统运行”日志信息。

日志管理员可以滚动查看，并可以在“日志类型”处选择希望查看的日志类型，列表中直接显示相应的日志类型。

还可以在“查找”右侧的文本框中输入查找关键字，然后点击“查找”按钮即可从列表中查找对应的日志信息。

2. 刷新日志

点击页面右上角的“刷新日志”，界面中显示系统当前缓存的管理员选择类型的日志信息。

3. 清空日志

点击页面右上角的“清空所有类型日志”，将删除系统缓存的所有类型的日志信息。

17.2.2 深度内容过滤日志

深度内容过滤日志指的是安全网关系统运行期间有关 HTTP 过滤、FTP 过滤、邮件过滤、DNS 过滤和命令过滤策略匹配情况等等的记录信息。

1. 查看日志

点击导航菜单 **日志与报警** > **日志查看**，并选择“深度内容过滤日志”页签，进入“日志查询”窗口，如下图所示。



界面中默认显示系统中所有缓存的所有 DPI 的日志信息。

日志管理员可以滚动查看，并可以在“日志类型”处选择希望查看的日志类型，列表中直接显示相应的日志类型。

还可以在“查找”右侧的文本框中输入查找关键字，然后点击“查找”按钮即可从列表中查找对应的日志信息。

2. 刷新日志

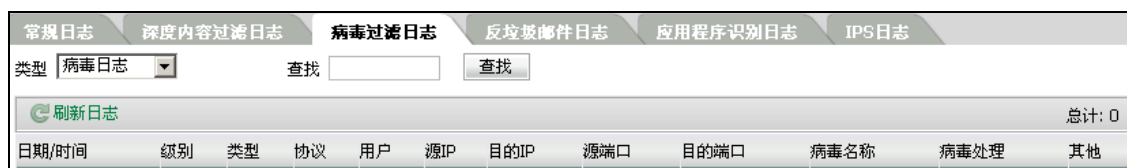
点击页面右上角的“刷新日志”，界面中显示系统当前缓存的管理员选择类型的日志信息。

17.2.3 病毒过滤日志

病毒过滤日志指的是安全网关系统运行期间有关病毒过滤策略匹配情况的记录信息。

1. 查看日志

点击导航菜单 **日志与报警** > **日志查看**，并选择“病毒过滤日志”页签，进入“日志查询”窗口，如下图所示。



界面中默认显示系统中所有缓存的所有病毒过滤的日志信息。

日志管理员可以滚动查看，并可以在“日志类型”处选择希望查看的日志类型，列表中直接显示相应的日志类型。

还可以在“查找”右侧的文本框中输入查找关键字，然后点击“查找”按钮即可从列表中查找对应的日志信息。

2. 刷新日志

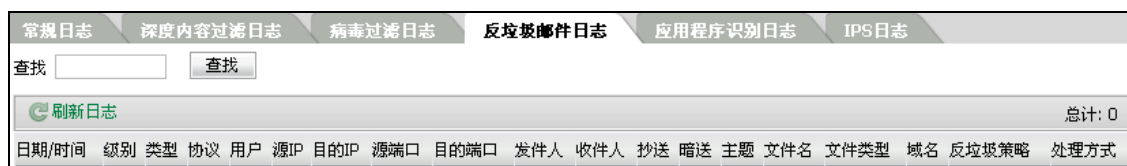
点击页面右上角的“刷新日志”，界面中显示系统当前缓存的管理员选择类型的日志信息。

17.2.4 反垃圾邮件日志

反垃圾邮件日志指的是安全网关系统运行期间有关反垃圾邮件模块过滤邮件情况的记录信息。

1. 查看日志

点击导航菜单 **日志与报警** > **日志查看**，并选择“反垃圾邮件日志”页签，进入“日志查询”窗口，如下图所示。



界面中默认显示系统中所有缓存的所有反垃圾邮件的日志信息。

日志管理员可以滚动查看，还可以在“查找”右侧的文本框中输入查找关键字，然后点击“查找”按钮即可从列表中查找对应的日志信息。

2. 刷新日志

点击页面右上角的“刷新日志”，界面中显示系统当前缓存的管理员选择类型的日志信息。

17.2.5 应用程序识别日志

应用程序识别日志指的是安全网关系统运行期间有关应用程序识别模块检测应用层数据情况的记录信息。

1. 查看日志

点击导航菜单 **日志与报警** > **日志查看**，并选择“应用程序识别日志”页签，进入“日志查询”窗口，如下图所示。

日期/时间	级别	类型	协议	源IP	目的IP	源端口	目的端口	源账号	Filter	动作	策略ID
总计: 0											

界面中默认显示系统中所有缓存的所有反垃圾邮件的日志信息。

日志管理员可以滚动查看，还可以在“查找”右侧的文本框中输入查找关键字，然后点击“查找”按钮即可从列表中查找对应的日志信息。

2. 刷新日志

点击页面右上角的“刷新日志”，界面中显示系统当前缓存的管理员选择类型的日志信息。

17.2.6 IPS 日志

用户可以通过 IPS 日志查询所有攻击事件及事件本身的详细内容，包括：排名、事件号、级别、次数及事件描述等等，从而了解当前网络受到攻击的具体状况。

具体步骤为：

1. 查看日志

选择 **日志与报警** > **日志查看**，并选择“IPS日志”页签，如下图所示。

时间	级别	事件号	次数	协议	源	目的	动作	事件描述
总计: 0								

界面中默认显示系统中所有缓存的所有 IPS 模块的日志信息。管理员可以滚动查看，还可以在“类型”处选择希望查看的日志类型，列表中直接显示相应的日志类型。

还可以在“关键字”右侧的文本框中输入查找关键字，然后点击“查找”按钮即可从列表中查找对应的日志信息。

2. 刷新日志

点击页面右上角的“刷新日志”，界面中显示系统当前缓存的管理员选择类型的日志信息。

17.3 报警

网络卫士安全网关具有完善的报警提示功能，支持邮件报警、NETBIOS 报警、声音报警、SNMP 报警、控制台报警五种报警方式。管理员首先需要添加报警规则，设置报警的对象和参数。然后设定触发报警规则的安全事件，包括设备本身发生故障和发生管理员预先定义的安全事件两种。这样当安全事件发生时，安全网关就会根据规则触发相应的报警信息。

17.3.1 添加报警规则

网络卫士安全网关支持以下几种报警方式：

- 邮件报警（发送电子邮件到用户指定的电子邮件地址）
- NETBIOS 报警（发送 NETBIOS 消息）：在接收 NetBios 消息的主机上必须启动 Messenger 服务。
- 声音报警（通过网络卫士安全网关的内置扬声器报警）
- SNMP 报警（通过发送 SNMP TRAP 消息到 SNMP 陷阱主机报警）
- 控制台报警（发送报警信息到 TOPSEC 管理中心）

安全网关的出厂配置中没有任何报警规则。设置报警规则的具体方法是：

- 1) 选择 **日志与报警 > 报警**，进入“报警设置”页面，如下图所示。

报警											
+ 添加 报警测试										总计: 2	
管理	系统	安全	策略	通讯	硬件	容错	测试	分类	名称	内容信息	操作
☐	☐	☐	☐	☐	☐	☐	☐	beep	test	长度:200 频率:440 延迟:100 重复:5	
☐	☐	☐	☐	☐	☐	☐	☐	console	test1		

- 2) 点击“添加”，打开报警配置窗口，如下图所示。

在“报警类型”选择报警方式：“邮件报警”、“声音报警”、“SNMP”、“NETBIOS”以及“控制台”，选择不同的报警方式将出现不同的参数项。

a) 选择“邮件报警”，界面如上图所示，界面参数说明如下表。

参数	说明
报警名称	用户指定的报警规则的名称。
服务器地址	要使用的发送邮件的 SMTP 服务器的 IP 地址。
服务器端口	SMTP 服务器端口号。
收件人地址	接收报警信息的电子邮件地址，如 abc@topsec.com.cn。
邮件主题	电子邮件主题。
身份认证	可选项，如果服务器要求验证用户身份后才会发送电子邮件，则必须选择此项。
发件人用户名	用于发送报警信息的电子邮件地址，必须是 SMTP 服务器的合法帐户。只有当选择了“身份认证”后，才能够设置该参数值。
用户密码	用户密码，发件人帐户对应的密码。只有当选择了“身份认证”后，才能够设置该参数值。

b) 选择“声音报警”，参数界面如下图所示。

报警服务规则

报警类型 声音报警

报警名称 *

声音报警 设为默认

输出频率 * [1-1000HZ]

发声长度 * [1-1000微秒]

重复次数 * [1-10次]

两次间隔 * [1-1000微秒]

确定
取消

参数说明如下表所示。

参数	说明
报警名称	用户指定的报警规则的名称。
设置为默认	如希望使用网络卫士安全网关的默认参数，可以点击“设置为默认”按钮，声音报警的各参数值自动显示为默认值，即输出频率为 440HZ、报警声音长 200 微秒、报警重复 5 次、两次报警间隔时间为 100 微秒。
输出频率	设置报警声音的频率，单位为 HZ，设定范围为 1-1000。
发声长度	设置报警声音延续的时间，单位为微秒，设定范围为 1-1000。
重复次数	设置报警声音重复多少次后停止，单位为次，范围为 1-10。
两次间隔	设置两次声音报警之间的间隔，单位为微秒，设定范围为 1-1000。

c) 选择“NETBIOS”报警，将弹出如下窗口。

报警服务规则

报警类型 NETBIOS

报警名称 *

主机名称 *

主机地址

确定
取消

参数说明如下：

参数	说明
报警名称	用户指定的报警规则的名称。
主机地址	要接受报警信息的主机的 IP 地址。 说明：

参数	说明
	接收 NetBios 消息的主机必须启动 Messenger 服务。
主机名称	要接受报警信息的主机的真实的名称。 说明： NetBios 主机命名要符合规范，只能由数字、字母、下划线“_”和中横线“-”组成，其他字符均为非法字符。

d) 选择“SNMP”报警，参数设置界面如下图所示。



报警服务规则

报警类型: SNMP

报警名称:

确定 取消

在“报警名称”处填写用户指定的报警规则的名称。

说明

- ◇ SNMP报警需要选择 **网络管理 > SNMP**，启动SNMP服务，并选择“陷阱主机”页签设置SNMP陷阱主机地址。具体操作请参见[4.2.4 SNMP](#)。

e) 选择“控制台”报警，参数设置界面如下图所示。



报警服务规则

报警类型: 控制台

报警名称:

确定 取消

在“报警名称”处填写用户指定的报警规则的名称。

3) 参数设置完成后，点击“确定”按钮，将该报警规则添加到安全网关中；点击“取消”按钮则取消此次操作，返回主界面。

说明

- ◇ 添加控制台报警后，需要启动系统监控功能：在 **系统管理 > 配置** 的“开放服务”页签中启动“监控服务”，并开放“MONITOR”服务，具体操作请参见[4.2.2.1 管理系统服务和4.2.2.2 开放服务](#)。

添加报警规则（例如 snmp 报警）后的界面如下图所示。

报警											
+ 添加		报警测试		总计: 2							
管理	系统	安全	策略	通讯	硬件	容错	测试	分类	名称	内容信息	操作
☐	☐	☐	☐	☐	☐	☐	☐	beep	beep	长度:200 频率:440 延迟:100 重复:5	 
☐	☐	☐	☐	☐	☐	☐	☐	snmp	snmp		

上图中规则红色框部分为触发该报警规则的安全事件，新添加的规则没有和任何安全事件关联，参数具体说明请参见[17.3.2 设置触发报警的安全事件](#)。蓝色框部分的内容为该报警规则的参数。

17.3.2 设置触发报警的安全事件

报警安全事件包括设备本身的故障和管理员定义的安全事件，如：

- 管理：指管理员对设备进行配置。
- 系统：用户登录、管理设备，系统启动或停止、系统升级、管理员进行日志设置、HA 状态切换、网络环路、网卡掉线等事件。
- 安全：系统根据 IDS 和 IPS 攻击策略监测到攻击发生。
- 策略：在添加访问控制策略时选择“系统报警”选项后，每当有匹配的访问控制策略起效时将会报警。
- 通讯：通过设备建立会话、会话断开、IP 地址冲突等关键通信事件。
- 硬件：系统 CPU、内存资源不足。
- 容错：系统恢复。
- 测试：用户对报警规则进行测试。

当成功添加一条报警规则到网络卫士安全网关后，还需要设置触发报警的安全事件。

设置方法是在已添加的报警规则的右侧窗口选择相应的安全事件，如下图所示。

报警											
+ 添加		报警测试		总计: 2							
管理	系统	安全	策略	通讯	硬件	容错	测试	分类	名称	内容信息	操作
☐	☒	☒	☐	☐	☒	☐	☒	beep	test	长度:200 频率:440 延迟:100 重复:5	
☐	☐	☐	☐	☐	☐	☐	☐	console	test1		

在上图报警规则中，安全事件选择了“系统”、“安全”、“硬件”和“测试”作为可触发报警的安全事件，在“分类”中可以看出报警方式采用的是声音报警。这条规则成

功设置后，当系统出现了“系统”、“安全”、“硬件”的事件时，就会触发一个报警，网络卫士安全网关会通过声音报警来提醒管理员。

说明

- ✧ 在添加由流量异常促发的报警安全事件时需要注意，由于流量异常根据四种情况（物理接口流量、协议组、协议比例和最大连接数）促发报警时产生的日志类型均为系统日志，但是它们触发报警的安全事件不是都为系统安全事件。其中物理接口流量超过阈值触发的报警安全事件为系统安全事件，协议组、协议比例和最大连接数超过阈值触发的报警安全事件为硬件安全事件。

点击“报警测试”，系统将按照设定的报警类型测试报警规则是否有效。

17.3.3 删除报警规则

点击待删除规则条目后的“删除”图标，弹出如下界面要求用户进行确认。



点击“确定”按钮，如果该规则没有关联的安全事件，则该规则删除成功；否则，不允许删除该规则，弹出错误提示框。

此时，用户需要首先清空该规则中关联的安全事件，然后才能够成功删除该规则。

附录 A 常用服务及端口

服务名称	端口号/协议	别名	说明
echo	7/tcp		
echo	7/udp		
discard	9/tcp	sink null	
discard	9/udp	sink null	
systat	11/tcp	users	#Active users
daytime	13/tcp		
daytime	13/udp		
qotd	17/tcp	quote	#Quote of the day
qotd	17/udp	quote	#Quote of the day
chargen	19/tcp	ttytst source	#Character generator
chargen	19/udp	ttytst source	#Character generator
ftp-data	20/tcp		#FTP, data
ftp	21/tcp		#FTP, control
telnet	23/tcp		
smtp	25/tcp	mail	#Simple Mail Transfer Protocol
time	37/tcp	Timserver	
time	37/udp	Timserver	
rlp	39/udp	resource	#Resource Location Protocol
nameserver	42/tcp	name	#Host Name Server
nameserver	42/udp	name	#Host Name Server
nicname	43/tcp	Whois	
domain	53/tcp		#Domain Name Server
domain	53/udp		#Domain Name Server
bootps	67/udp	dhcps	#Bootstrap Protocol Server
bootpc	68/udp	dhcpc	#Bootstrap Protocol Client

服务名称	端口号/协议	别名	说明
tftp	69/udp		#Trivial File Transfer
gopher	70/tcp		
finger	79/tcp		
http	80/tcp	www www-http	#World Wide Web
kerberos	88/tcp	Krb5 kerberos-sec	#Kerberos
kerberos	88/udp	Krb5 kerberos-sec	#Kerberos
hostname	101/tcp	hostnames	#NIC Host Name Server
iso-tsap	102/tcp		#ISO-TSAP Class 0
rtelnet	107/tcp		#Remote Telnet Service
pop2	109/tcp	postoffice	#Post Office Protocol – Version 2
pop3	110/tcp		#Post Office Protocol – Version 3
sunrpc	111/tcp	Rpcbind portmap	#SUN Remote Procedure Call
sunrpc	111/udp	Rpcbind portmap	#SUN Remote Procedure Call
auth	113/tcp	Ident tap	#Identification Protocol
uucp-path	117/tcp		
nntp	119/tcp	usenet	#Network New Transfer Protocol
ntp	123/udp		#Network Time Protocol
epmap	135/tcp	Loc-srv	#DCE endpoint resolution
epmap	135/udp	Loc-srv	#DCE endpoint resolution
netbios-ns	137/tcp	nbname	#NETBIOS Name Service
netbios-ns	137/udp	nbname	#NETBIOS Name Service
netbios-dgm	138/udp	nbdatagram	#NETBIOS Datagram Service
netbios-ssn	139/tcp	nbssession	#NETBIOS Session Service
imap	143/tcp	imap4	#Internet Message Access Protocol
pcmail-srv	158/tcp		#PCMail Server
snmp	161/udp		#SNMP
snmptrap	162/udp	Snmp-trap	#SNMP trap
print-srv	170/tcp		#Network PostScript

服务名称	端口号/协议	别名	说明
bgp	179/tcp		#Border Gateway Protocol
irc	194/tcp		#Internet Relay Chat Protocol
ipx	213/udp		#IPX over IP
ldap	389/tcp		#Lightweight Directory Access Protocol
https	443/tcp	MCom	
https	443/udp	Mcom	
microsoft-ds	445/tcp		
microsoft-ds	445/udp		
kpasswd	464/tcp		# Kerberos (v5)
kpasswd	464/udp		# Kerberos (v5)
isakmp	500/udp	ike	#Internet Key Exchange
exec	512/tcp		#Remote Process Execution
biff	512/udp	comsat	
login	513/tcp		#Remote Login
who	513/udp	whod	
cmd	514/tcp	shell	
syslog	514/udp		
printer	515/tcp	spooler	
talk	517/udp		
ntalk	518/udp		
efs	520/tcp		#Extended File Name Server
router	520/udp	Route routed	
timed	525/udp	timeserver	
tempo	526/tcp	newdate	
courier	530/tcp	rpc	
conference	531/tcp	chat	
netnews	532/tcp	readnews	
netwall	533/udp		#For emergency broadcasts

服务名称	端口号/协议	别名	说明
uucp	540/tcp	uucpd	
klogin	543/tcp		#Kerberos login
kshell	544/tcp	krcmd	#Kerberos remote shell
new-rwho	550/udp	new-who	
remotefs	556/tcp	rfs rfs_server	
rmonitor	560/udp	rmoitord	
monitor	561/udp		
ladps	636/tcp	sldap	#LDAP over TLS/SSL
doom	666/tcp		#Doom Id Software
doom	666/udp		#Doom Id Software
kerberos-adm	749/tcp		#Kerberos administration
kerberos-adm	749/udp		#Kerberos administration
kerberos-iv	750/udp		#Kerberos version IV
kpop	1109/tcp		#Kerberos POP
phone	1167/udp		#Conference calling
ms-sql-s	1433/tcp		#Microsoft-SQL-Server
ms-sql-s	1433/udp		#Microsoft-SQL-Server
ms-sql-m	1434/tcp		#Microsoft-SQL-Monitor
ms-sql-m	1434/udp		#Microsoft-SQL-Monitor
wins	1512/tcp		#Microsoft Windows Internet Name Service
wins	1512/udp		#Microsoft Windows Internet Name Service
ingreslock	1524/tcp	ingres	
12tp	1701/udp		#Layer Two Tunneling Protocol
pptp	1723/tcp		#Point-to-point tunneling protocol
radius	1812/udp		#RADIUS authentication protocol
radacct	1813/udp		#RADIUS accounting protocol
nfsd	2049/udp	nfs	#NFS server
knetd	2053/tcp		#Kerberos de-multiplexor

服务名称	端口号/协议	别名	说明
man	9535/tcp		#Remote Man Server

附录 B 简单网络管理协议 SNMP

SNMP（Simple Network Management Protocol，简单网络管理协议）首先是为了解决 Internet 上的路由器管理问题由 IETF 的研究小组而提出的，设计原则是简单性和扩展性。简单性是体现在信息类型的限制、请求响应或协议等，扩展性是通过将管理信息模型与协议、被管理对象的详细规定（MIB）分离实现的。

SNMP 网络管理模型包括以下部件：管理站、代理者、管理信息库、网络管理协议。

管理站一般是一个独立的设备，也可利用共享系统。管理站是网络管理员与网络管理系统的接口，基本构成为：一组具有分析数据、发现故障等功能的管理程序；一个用于监控网络的接口；一个从被管网络实体的 MIB 中抽取信息的数据库。

代理者负责应答来自管理站的信息请求和动作请求进行，并随机地向管理站报告一些重要的意外事件。如主机、网桥、路由器及集线器等装备了 SNMP 的平台均可作为代理者。

网络资源被抽象为对象，SNMP 中的对象是表示被管资源某一方面的数据变量，被标准化为跨系统的类，对象集合组织为管理信息库（MIB）。MIB 作为设在位于代理者的管理站访问点的集合，管理站通过读取 MIB 中对象的值来进行网络监控。管理站可以在代理者处产生动作，也可以通过修改变量值改变代理者处资源的配置。

管理站和代理者之间通过网络管理协议通信，SNMP 通信协议支持：管理站读取代理者处对象的值、管理站设置代理者处对象的值、代理者向管理站通报重要事件。

一般地，应至少要有两个系统能够完成管理站功能，以提供冗余度，防止故障。

网络卫士系列安全网关支持 SNMP 管理，本附录通过 OpenView SNMP 管理软件为例，介绍如何通过 SNMP 客户端管理网络卫士系列安全网关。

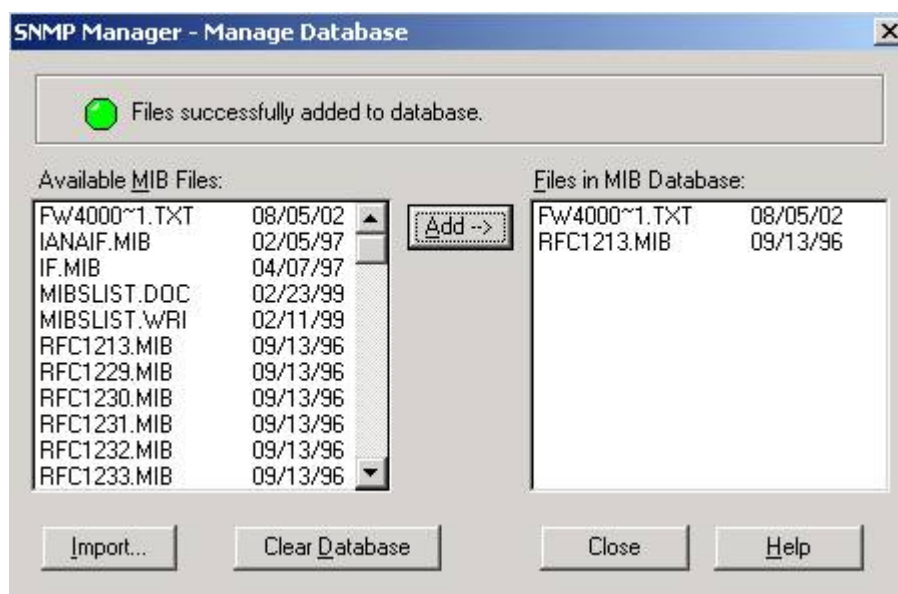
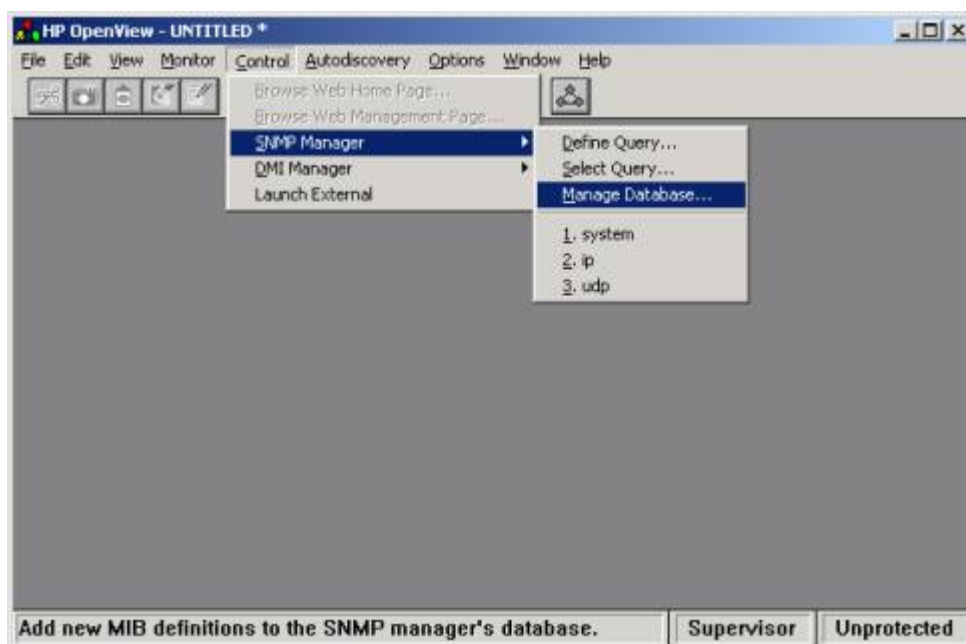
本附录内容主要包括：

- 如何导入 MIB 库。
- 如何定义查询。
- 如何执行和取值查询。

1. 导入 MIB 库

OpenView 已经包含了基本 mib-2 组信息，只需要导入网络卫士系列安全网关-MIB 模块信息就可以了，假设存放位置为 d:\wyd\snmpconf\snmp\TOPSEC-MIB.TXT。

打开 OpenView，如下图，选中 **Control > SNMP Manager > Manage Database**。



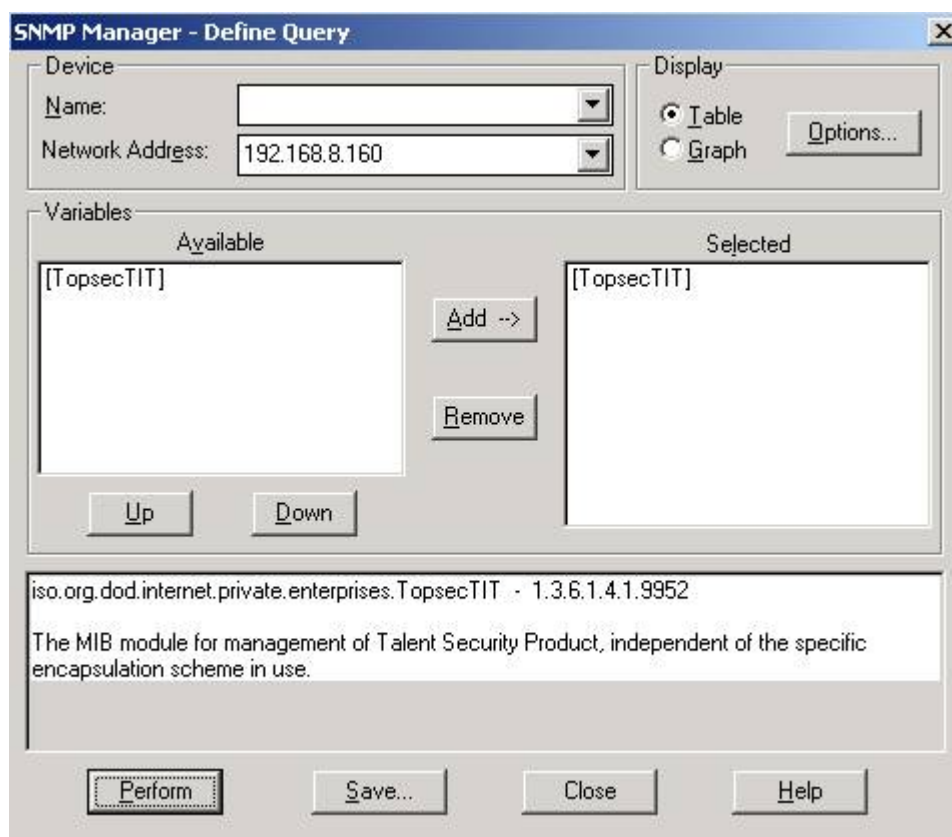
将出现如上图所示对话框，左边是可用的 MIB 库，右边是已导入的 MIB 数据库。

点击“Import”按钮，出现如下对话框，选择 d:\OV\MIBS\TOPSEC-MIB.TXT，点击“确定”即可。此时 TOPSEC-MIB.TXT 便出现在上图的左边边框中。然后，选中上图中的“TOPSEC-MIB.TXT”，点击中间的“Add->”按钮。稍候，便将 TOPSEC-MIB.TXT 文件成功导入到 MIB 库中。



2. 定义查询

如下图所示，打开**Control > SNMP Manager > Define Query**，进入如下图所示的对话框。



Network Address 栏中填入 SNMP 服务器（代理）IP 地址，在 Available 栏中选中要查询的变量名。如上图所示，选中[vpnMIBObjects]，状态栏将显示 vpnMIBObjects 在 MIB 库中的位置：

iso.org.dod.internet.private.enterprises.FW4000-MIB.NetSecurity.vpnMIBObjects-.1.3.

6.1.4.1.9952.1.2。选中后，点击“Add-->”，变量[vpnMIBObjects]将出现在右边的 Selected 栏中。如果同时查询其他的变量，请按照以上操作继续选择要查询的变量。如上图所示，

已经选中了两组变量，其中“[]”内的变量是 MIB 树形结构中的非叶子节点，双引号“”内的变量是叶子节点。

选定变量后，定义显示方式。在右上角的 Display 栏中选中 Table 显示方式（大多数变量可选择表格形式显示，这是因为这些变量值一般不会变化）或者 Graph 显示方式（实时变化的变量，例如 CPU 的利用率）。

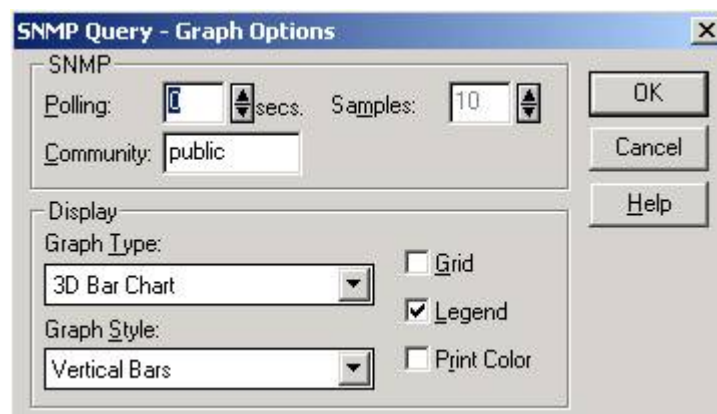
如果选择 Table 表格显示方式，然后点击“Options”按钮，进入如下图所示的对话框：



- **设置Polling值** 对于值不断变化的变量，请在Polling栏中设置适当的值，SNMP 客户机（管理者）每隔一个Polling时间，轮询一次SNMP服务器（代理），获取最新变量值。如果变量值是不变的，请将Polling值设置为 0。
- **设置Community值** 如果是SNMP网络用户，Community栏中填入SNMP网络用户口令；如果是SNMP管理员，Community栏中则填入SNMP管理员口令。
- **设置Set Community值** Set Community是指设置变量值的口令，这里所指的所有变量仅能查询，因此无需设置Set Community值。

设置完成后，点击“OK”确定。

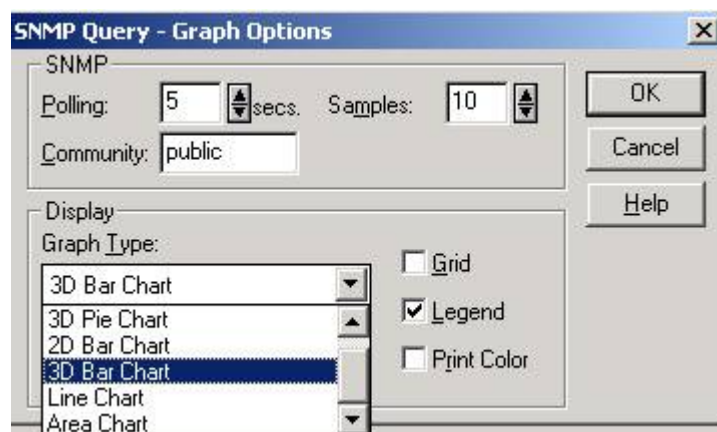
如果选择 Graph 图形显示方式，然后点击“Options”按钮，进入如下图所示的对话框。



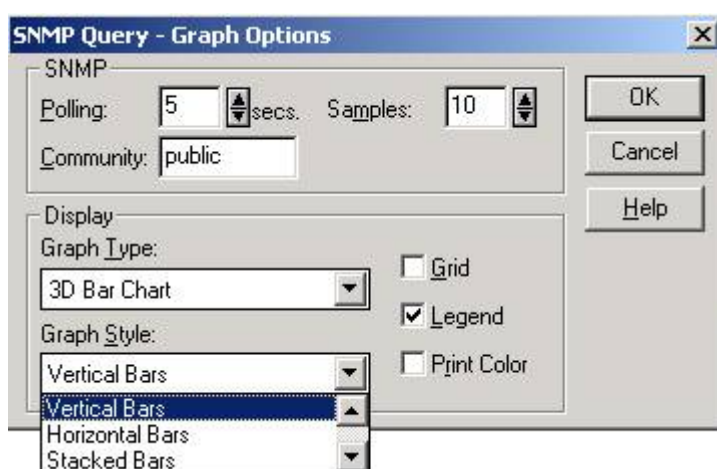
设置 Polling 值 如表格方式。

设置 Community 值 如表格方式。

选择 Graph Type 如下图所示，在 Graph Type 下拉菜单中选中图形类型。



选择 Graph Style 如下图所示，在 Graph Style 下拉菜单中选择图形风格。

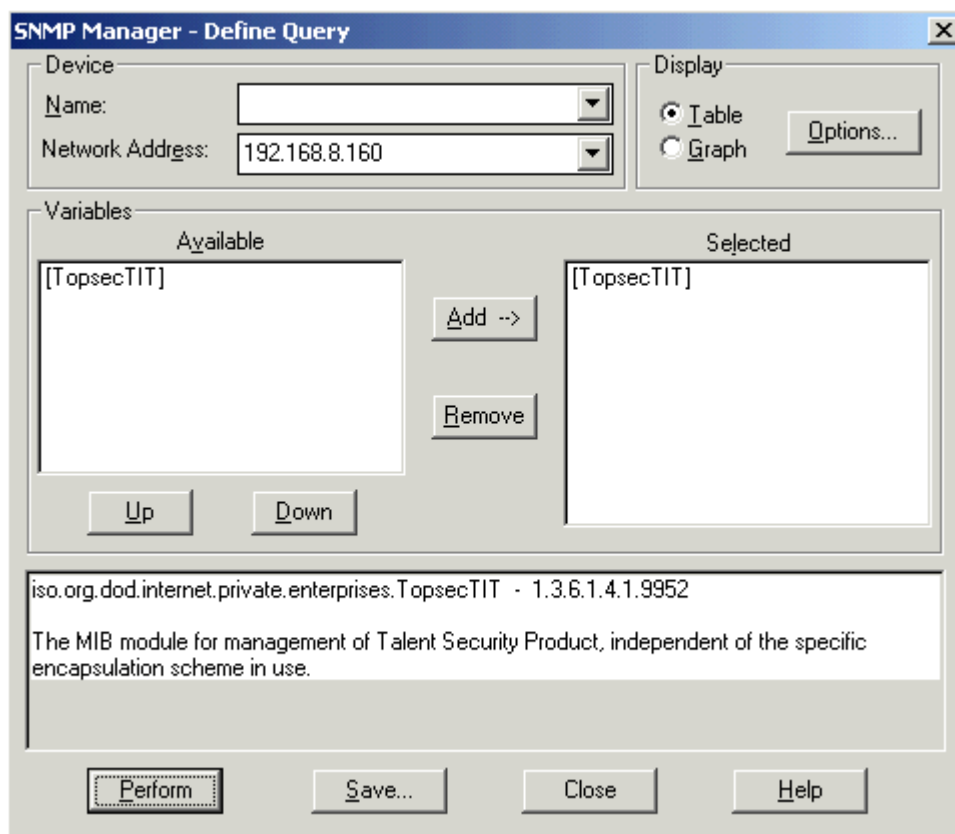


设置完成后，点击“OK”确定。

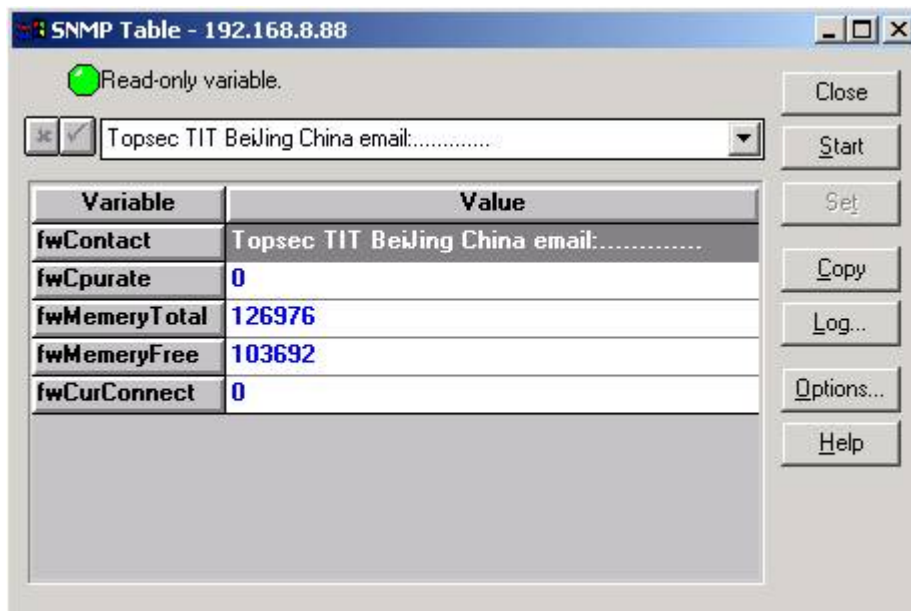
3. 执行查询取值

定义查询后，就可执行查询了。假设定义了一组变量 [fwdevicestatus]，选择 Table 表格显示方式。

打开**Control > SNMP Manager > Define Query**，进入如下图所示的对话框。



此时，点击左下方的“Perform”按钮，将弹出如下图所示的查询结果界面。



最上面的一栏是第一个查询结果。下面是变量名和变量值的对照表。右边是控制按钮。

对于 Graph 图形方式类似，在此省略。

说明

-
- ✧ 不要将任何口令（community）设置为 public，因为在使用 OpenView 访问 SNMP 代理时，如果 community 栏为空，则 OpenView 以默认字符串 public 进行访问，这样即使不知道口令的用户，同样可以访问到 SNMP 代理。
-

附录 C 术语索引

这里集中对出现在帮助查看程序中的专业术语进行了详细的解释,用户根据需要了解的专业术语的开头字母,在左边的术语目录中找到相关项,单击术语项即可显示出对该术语的详细解释。

A

安全服务网络 SSN

特指用户网络中对外提供服务的服务器网络,这些服务包括 Web、FTP 等。传统的网络区域划分,如 DMZ 隔离区,一般把对外服务网络作为内网的一部分。

网络卫士安全网关支持的三接口划分方法与之不同,提供了更好的安全保护。除了 SSN 与外网之间有防火墙保护,而且 SSN 与内网之间也有防火墙保护,一旦 SSN 受到攻击和破坏,内网络仍会处于防火墙的保护之下。

安全服务器网络(SSN)技术支持 SSN 主机的单独管理,和通过 FTP 等方式的内网管理。

安全联盟 SA

在 IPSec 协议中,一个安全联盟 SA (Security Association) 是关于 IPSec 通信双方在单向通信时采用的安全参数的一个协定,一个双工 IPSec 安全隧道,至少需要两个 SA。

一个 SA 组主要由以下部分构成:

加密、验证算法和密钥;

密钥管理方法(自动 IKE 或系统管理员手工配置);

SA 的生命周期,可以增强 IPSec 安全性。

B

包过滤

一种在网络层对数据包进行分析过滤的网络安全访问策略,防火墙通过分析每个数据包的源地址、源端口、目的地址、目的端口号、协议状态等网络层信息特征,过滤网络数据包。

半连接

一个正常的 TCP 连接需要三次握手:首先客户端发送一个包含 SYN 标志的数据包,其后服务器返回一个 SYN/ACK 的应答包,表示客户端的请求被接受,最后客户端再返回一个确认包 ACK,这样才完成 TCP 连接。在服务器端发送应答包后,如果客户端不发出确认,服务器会等待到超时,这期间这些半连接状态都保存在一个空间有限的缓存队列中。这类未完成三次握手协议的非正常 TCP 连接,在网络卫士安全网关中,称之为半连接。

D

带宽策略

带宽策略是一种用于限制网络节点或子网之间通信可用带宽的策略规则，可以防止用户滥用带宽，限制某个防火区域、节点或子网的用户可用的最大带宽。同时带宽策略还可在带宽资源紧张的情况下，保证关键应用的带宽。本版本支持的带宽策略是一种分层的带宽管理策略。

地址转换策略

地址转换策略是一种描述防火墙如何修改数据包报文规则的策略，网络卫士安全网关支持三种地址转换策略：不作转换，源地址转换和目的地址转换。其中不作转换是缺省地址转换策略。

地址对象

这里的对象指的是网络对象。网络卫士安全网关的管理是基于对象的，所有的策略（规则）都通过对象来定义，在配置访问规则、地址转换策略等规则之前，必须预先定义相关的所有对象。例如，为了限制某台主机的访问，必须预先定义包括这台主机的对象，可以是子网、范围等对象。

地址组对象

对象组中可以包含多个网络节点或子网对象。在网络卫士安全网关中，对象组可以作为定义规则的源或目的。

端口映射

是一项将目标主机的服务端口映射到防火墙接口的某一个端口的技术，主要用于外部主机访问位于内部网络的服务器。在防火墙中，将防火墙外网网卡的某一个端口映射到内部的某台服务器的一个服务端口，外网用户只需访问防火墙外网接口的特定端口即可获得内部服务器的相应服务。

端口映射可以解决网络公共地址短缺的问题，同时由于端口映射只映射内部服务器的单一需要提供对外服务的端口，可保证该服务器的服务单一性。另外，由于用户并不直接访问内部网络中的服务器而是通过防火墙转发，且防火墙只将数据包转发到指定内部地址的指定端口，所以可有效保护内部网络安全。

DHCP

DHCP，即 Dynamic Host Configuration Protocol，动态主机配置协议，是 Internet 网络工程师任务小组（IETF）设计的，目的是减轻 TCP/IP 网络的规划、管理和维护的负担，解决 IP 地址空间缺乏等问题。DHCP 提供了一个动态指定 IP 地址和配置参数的机制，即当一台设置为自动获取 IP 地址的计算机在登录网络时，会向网络上发送租用 IP 地址的请求，专门负责提供 IP 地址的 DHCP 服务器回应这个请求，为这台计算机提供一个空闲的 IP 地址。

DHCP 中继

是一项支持某一网段的主机连接到位于另一网段的 DHCP 服务器，获取 DHCP 服务的网络技术。

深度过滤

是深度报文检测（DEEP PACKET INSPECTION）的缩写，网络卫士安全网关可以通过深度过滤对应用层的访问进行内容过滤，从而实施更细粒度的访问控制。目前网络卫士安全网关支持的深度过滤包括：关键字、文件、FTP、HTTP、POP3、SMTP。

多播组

是网络卫士安全网关的一个特殊对象，主要用于定制允许 IP 多点广播数据报文穿越网络卫士安全网关。在网络卫士安全网关中，如果允许 IP 多点广播数据报穿越防火墙，可以通过定义一个相关的多播组对象实现。需特别说明的是，一个多播组对象所覆盖的防火区域必须位于一个透明网络内。

F

防火区

表示防火墙的某个接口控制的网络区域。防火区与网段有所不同，可以将整个网络看成由某台防火墙分割开的几个防火区，每个防火区可以包含一个或多个网段。与区域概念也有所不同，可以把一个防火区看成是一个区域，区域可以包含多个防火区，如全局区域。

访问权限

是网络卫士安全网关借鉴文件系统的访问权限设计的网络访问控制技术，目前支持三种访问权限，且支持访问权限组合：

读权限：表示将数据从服务器（或区域）读出去。例如 FTP 中的取文件，HTTP 中的取网页，POP3 中的收邮件。

写权限：表示将数据写到服务器（或区域）上。例如 FTP 中的上传文件，SMTP 中的发邮件。

执行权限：表示可以执行服务器（或区域）上的程序或 CGI。

访问策略

是用户可自定义的一种允许或禁止数据包通过防火墙的策略规则，每一个访问策略中包含的信息主要包括：数据包的源地址、目的地址、协议（服务类型）以及对满足条件的数据包进行何种操作（转发或丢弃）。网络卫士安全网关支持四种用户可定义的访问策略：包过滤策略、文件过滤策略、HTTP 过滤策略和邮件过滤策略。

分片策略

在一些特殊情况下，用户需要根据网络应用的实际情况设置接口的最大传输单元值，即 MTU。如果两个接口所设的 MTU 值不一致，为了防止转发丢包则需要分片重组，即防火墙根据对方接口 MTU 值重新分片组合同一连接的多个数据包，并转发。网络卫士安

全网关中，分片策略是指不对两个网络对象之间的通信进行分片重组，分片策略可以提高网络通信的效率。

G

管理端口

是指通过集中管理器配置管理网络卫士安全网关采用的通信端口，网络卫士安全网关中缺省的管理端口为 4000，本版本支持用户自定义管理端口，用户可以根据实际网络需求，修改安全网关的管理端口。只有重新启动安全网关后，修改的管理端口才能生效。

H

H323

H323 是国际电信联盟（ITU-T，Internet Telecom Union）发布的一项局部网络视频会议标准，定义了分组网（LAN， WAN， Internet）上进行多媒体通信所需的组件、协议和规程。

负载均衡组

是指在某个防火区域中定义的由服务器作为节点的一个对象组。在通信策略中，可以使用负载均衡组来控制其他主机对负载均衡组中服务器的访问。

混合模式

网络卫士安全网关的一种工作模式，这种模式是透明模式和路由模式的混合，即安全网关的某些区域（接口）工作在透明模式下，而其他的区域（接口）工作在路由模式下。该模式的应用可以使安全设备更好的适应复杂网络情况。

I

IKE

是 Internet 密钥交换协议，主要用于在两个 IPSec 对等体间协商一条 IPSec 隧道的协议。IKE 协议由三个不同的协议组成：

SKEME：实现公密加密认证机制。

Oakley：基于两个对等体间的加密密钥机制。

ISAKMP：定义消息交换体系结构，包括 IPSec 对等体间分组形式和状态转换。

IPSEC

是一个定义在 IP 层实现安全加密通信机制的协议族，IPSec 协议为敏感数据通过非安全网络区域（如 Internet）安全传输提供解决方案。IPSec 包含两个主要协议：认证头（AH）协议和负载安全封装（ESP）协议，AH 协议主要用于数据源和数据完整性验证，并提供局部顺序完整性检验，防止重传攻击；ESP 协议同时提供身份验证和 IP 通信机密性保护。

J

节点

又称为网络节点，表示某个区域中的一台物理机器。它可以作为访问策略中的源和目的，也可以作为地址转换策略中的源和目的。例如网络中有一台 HTTP 服务器，则可以定义一个网络节点为“HTTP_SERVER”，同时说明一条访问策略，表示其他区域的机器对这台服务器的访问权限。网络节点同时可以作为地址映射的地址池使用，表示地址映射的实际机器。

接口

在网络卫士安全网关中，接口与通用的网络接口有所不同。网络卫士安全网关的接口主要有两种：

物理接口，和安全网关的物理端口一一对应，如 Eth0。

逻辑接口，也就是全局接口（Global），是所有物理接口的总称。

在网络卫士 ARES 防火墙中，每个接口和防火区域之间的关联是固定的，对应关系如下：

Eth0: SSN 安全服务网络

Eth1: 外网

Eth2: 内网

僵死连接

是指通信双方保持连接状态，但在一段时间内不存在数据交换的连接。网络卫士安全网关提供了启用僵死连接功能，用户可设置僵死连接的保留时间及最大数目，在某些特殊应用环境下保留已建连接，可以提高防火墙的性能。

静态路由

与标准静态路由不同，网络卫士安全网关提供的静态路由不是只根据目的地址，而是根据目的地址和源地址进行路由。基于源和目的地址的路由定义方式可以实现内部网络的指定对象使用特定外部线路与外部网络通信，进一步增强了网络的通信安全。

L

Land 攻击

是一种 DOS 攻击，基本原理是把请求数据报文中的客户端的 IP 和端口设为主机的 IP 和端口，发送给主机，使得主机给自己发送 TCP 请求和连接，造成目标机解析 Land 包占用太多资源，从而使资源消耗光，导致宕机。这种伪装对一些身份认证系统的威胁是巨大的。

路由模式

网络卫士安全网关的一种工作模式。在这种模式下，防火墙类似于一台路由器转发数据包，将接收到的数据包的源 MAC 地址替换为相应接口的 MAC 地址，然后转发。该模式适用于每个区域都不在同一个网段的情况。和路由器一样，防火墙的每个接口均要根据区域规划配置 IP 地址。

M

目的地址转换

即把安全设备的接口地址或某个指定 IP 与内部主机地址之间建立一种映射关系。当外部用户试图访问内部主机提供的服务时，用户访问的地址是映射的防火墙接口地址，防火墙将用户服务请求转发给提供服务的内部主机，从而达到保护内部主机的目的。

网络卫士安全网关支持地址映射和端口映射。地址映射是直接把防火墙的接口 IP 地址与目标主机 IP 地址进行映射；端口映射则是将目标主机的服务端口映射到防火墙接口的某一个端口。

MMS

MMS（Media Server Protocol）由微软定义的一种流媒体传输协议。流媒体就是指在网络上使用流式传输技术连续传输时的基媒体，是通过网络传输的音频、视频或多媒体文件。

MIB 管理信息库

是网络管理协议 SNMP 访问的管理对象数据库，包括 SNMP 可以通过网络设备的管理代理进行设置的变量。MIB 采用树形结构支持两种方式访问 MIB 对象值：一种是快速访问，另一种慢速访问。快速访问时只须输入一些数据，慢速访问在需要附加其它信息。SNMP MIB 的对象定义十分严格，指定了对象的数据类型、允许的形式、取值范围和与其它 MIB 对象的关系。

MTU 最大传输单元

Maximum Transmission Unit, TCP/IP 通信中，每一个网络接口都定义了一个最大传输单元，描述可以通过的数据包的最大尺寸。如果一个数据包大于接收方的 MTU 值时，系统将其划分成多个小的数据包（称之为 IP 碎片）来传输，接收方则会将这些 IP 碎片重组还原整个数据包。

O

OSPF

OSPF（Open Shortest Path First），开放最短路径优先协议。OSPF 是一种典型的链路状态路由协议。采用 OSPF 的路由器彼此交换并保存整个网络的链路信息，从而掌握全网的拓扑结构，独立计算路由。目前广为使用的是 OSPF 第二版，最新标准为 RFC2328。

OTP

即一次性口令认证（One Time Password），网络卫士安全网关内置基于 Lamport's Hash 协议的 OTP 数据库，利用 HASH 算法的不可逆性构造了一系列用户口令的 HASH 值，并把口令的 HASH 值代替明文口令存储在数据库中。每当完成一次用户认证，OTP 数据库中的用户口令就会被一个新的 HASH 值所取代，即使数据库的内容泄漏，攻击者也不能根据 OTP 数据库的内容获得用户的有用信息。在网络卫士安全网关中，HASH 算法采用的是 MD5。

P

PUDP 协议

PUDP（Pseudo-User Datagram Protocol）伪用户数据报协议，主要用于解决 IPSec 报文通过 NAT 和防火墙的问题，并不为 IP 报文提供额外的安全服务，作为一个可选的功能由 IKE 在进行密钥交换时与远程 VPN 实体进行协商。

Ping Flood

一种 Dos 攻击，基本原理是通过发送大量的 Ping 指令到目标系统，在 Ping 指令上使用了伪装的 IP 地址。由于目标系统尝试回应这些使用假冒地址的服务请求，导致耗用大量系统资源，最终目标系统陷入瘫痪。

Ping Sweep

即 Ping 扫描，是一种网络攻击，通过对一个网段进行大范围的 Ping，由此可确定这个网段的网络运作情况。

Ping of death

一种 Ping 攻击，通过向目标端口发送大量的超大尺寸的 ICMP 包来实现的。在早期的阶段，路由器对所传输的文件包最大尺寸都有限制，许多操作系统对 TCP/IP 的实现规定 ICMP 包的最大尺寸为 64KB，且在对包的标题头进行读取后，要根据该标题头里包含的信息来为有效载荷生成缓冲区。一旦产生出现畸形包，即声称尺寸超过 ICMP 上限的包，也就是加载的尺寸超过 64KB 上限时，就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，致使接受方死机。

Q

区域

在网络卫士安全网关中，把区域看作是一段具有相似安全属性的网络空间。在区域的划分上，网络卫士安全网关的区域和接口并不是一一对应的，也就是说一个区域可以包括多个接口。但是反过来，每个物理接口只能属于一个区域，也就是说每个接口所控制的网络只能具有一种安全属性。

缺省网关

即缺省路由。当在特殊数据包中，路由器无法找到目的地址，则将数据包通过一个缺省路由发送到另一路由器，称之为缺省路由。

缺省访问权限

主要用于对于接收的数据包不存在可匹配的访问策略时，网络卫士安全网关对数据包的处理缺省处理规则。支持定义如下的缺省访问权限：

没有任何权限，即如果找不到相匹配的访问策略，则禁止访问。

可读，即如果找不到相匹配的访问策略，而这次访问的目的是想从本区域将数据读出去，则允许访问。

可写，即如果找不到相匹配的访问策略，而这次访问的目的是想将数据写到本区域，则允许访问。

可执行，即如果找不到相匹配的访问策略，而这次访问的目的是想执行服务器（或区域）上的程序或 CG，则允许访问。

其中可读、可写可以合并，表示允许任何访问。

缺省日志选项

对此防火区域访问时的缺省日志选项。当外界的访问找不到相匹配的访问策略时，执行缺省访问权限，同时采用缺省的日志选项。

R

Radius

The Remote Authentication Dial-In User Service（Radius）认证协议，网络卫士安全网关支持的一种第三方认证机制。协议要求用户进行认证请求时，不仅要提供用户名和密码，而且必须知道用户和 Radius 数据库之间的共享密钥。当用户试图登录防火墙时，防火墙将用户提供的信息送到 Radius 数据库进行比较。在认证过程中，交互信息采用 MD5 加密算法。

认证

是一种确认通信中通话双方（用户或者网络设备）身份的机制。业界支持的认证标准很多，不同的认证方式通常会采用一个或多个认证数据库来存储认证信息，如用户名、密码、令牌、或者数字证书等。不同的认证机制所采用的算法和认证步骤也不尽相同。

网络卫士安全网关除了自带的认证数据库外，还支持本地的多种认证服务器或者远程第三方认证。网络卫士安全网关支持的认证机制包括 Redius、 TACACS+、 SecurID、 VieCA、 VRC、 OTP 等。

在网络卫士安全网关中，认证机制主要应用在两个方面：防火墙的登录认证和 VPN 通信认证。

认证服务器

一般来说，每种认证协议均使用一个独立的数据库存储用户信息。安装认证数据库的主机被称为认证服务器。

RTP

RTP（Routing Information Protocol），路由信息协议。RIP 只保留到目的地的最佳路由，当一条交换过来的新的路由信息提供了一条更佳的路由时，RIP 就用它来替换旧的信息。当网络拓扑改变是，RIP 实体会向外发布路由更新报文，以便与其他网络设备共享。每一个路由器收到一条更新报文后除了更新自己的路由表之外，还接着传播这条报文，这可以简单地理解为互通有无、彼此信任。

PTSP

RTSP（Real Time Streaming Protocol），实时流通讯协议，是 RealNetworks 公司协助建立的一个用来传送实时流媒体的开放标准。

S

SecurID

Security Dynamics Client/Server Protocol 协议，网络卫士安全网关支持的一种第三方认证机制。认证时不仅要求用户提供个人身份码（PIN），而且还要求提供一个一次性令牌。通常，这个令牌存储在一张带有液晶显示的 8 位智能卡上。每次登录，智能卡都会产生一个随机数作为令牌，供用户进行认证。随机数是由一个 RSA 提供的算法产生的，非常安全。

生成树协议

在交换网络环境中，为了能够有效地传输流量和保证网络的可靠性，往往需要提供冗余和故障快速恢复功能。在网络中通常设置了一些冗余链路，这些冗余链路可能导致物理网络拓扑结构中存在环路。由于交换机不能像路由器那样知道报文可以经过多少次转发，一旦网络中存在环路，就会造成报文在环路内不断循环和增生，可能出现“广播风暴”，导致网络不可用。

生成树协议主要是用于解决可能出现的“广播风暴”，基本思想是：让网络像树一样的生长，通过有选择地阻塞网络冗余链路来消除网络二层环路，同时保留链路备份功能。树的构造算法被称为生成树算法（SPA，Spanning Tree Algorithm）。

SSH

SSH 全称 Secure SHell。SSH 是一个用来替代 TELNET、FTP 以及 RLOGIN、RSH 和 RCP 命令的工具包，主要是解决口令在网上明文传输的安全问题。

从 SSH 客户端提供两种级别的安全验证：

第一种级别基于口令的安全验证。只要知道自己帐号和口令，就可以登录到远程主机。所有传输的数据都会被加密，但是不能保证正在连接的服务器就是用户想连接的服务器。可能会有别的服务器在冒充真正的服务器。

第二种级别基于密匙的安全验证。需要依靠密匙，也就是必须为每个登录用户创建一对密匙，并把公用密匙放在需要访问的服务器上。如果用户要连接到 SSH 服务器上，客户端软件就会向服务器发出请求，请求用登录用户的密匙进行安全验证。服务器收到请求之后，先在该服务器的相关目录下寻找该用户公密，然后把它和接收到的用户公密进行比较。如果一致，服务器就用公匙加密“质询”（challenge）并把它发送给客户端软件。客户端软件收到“质询”之后就可以用的私匙解密再发送给服务器，从而实现保密通信。

Smurf 攻击

一种 Dos 攻击，基本原理是通过把 ICMP 应答请求数据包的回复地址设置成受害网络的广播地址，导致该网络的所有主机都对此 ICMP 应答请求作出回复，导致网络阻塞。

Smurf 攻击比 Ping of death 攻击的流量高出一到两个数量级。更加复杂的 Smurf 攻击则是将源地址改为第三方网络的广播地址，最终导致第三方崩溃。

SYN FLOOD

一种 Dos 攻击，基本原理是利用服务器的连接缓冲区漏洞，通过向服务器不断地成倍发送只有 SYN 标志的 TCP 连接请求。当服务器接收时，认为是没有建立起来的连接请求，于是为这些请求建立会话，放入缓冲区队列。如果 SYN 请求超过了服务器容量的限制，即缓冲区队列溢出，那么服务器将不再接收新的请求，导致其他合法用户的连接都被拒绝。

SNMP 网络管理协议

SNMP (Simple Network Management Protocol, 简单网络管理协议) 是由 IETF 的研究小组而提出的，主要用于解决 Internet 上的路由器管理问题，此协议包括了监视和控制变量集以及用于监视设备的两个数据格式：SMI 和 MIB。

SNMP 网络管理包含以下几个重要部分：管理基站、管理代理、管理信息库和网络管理协议。管理基站通常是一个独立的设备，它用作网络管理者进行网络管理的用户接口。基站上必须装备有管理软件，同时应该具备将管理命令发出基站的能力。管理代理是一种网络设备，如主机、网桥、路由器和集线器等。这些设备能够接收管理基站发来的信息，它们的状态是管理基站可监视的。管理代理响应基站的请求，也可以在没有请求的情况下向基站发送信息。MIB 是对象的集合，代表网络中可以管理的资源和设备。每个对象基本上是一个数据变量，它代表被管理的对象的一方面的信息。管理站和代理者之间通过网络管理协议通信，SNMP 通信协议支持：管理站读取代理者处对象的值；管理站设置代理者处对象的值；代理者向管理站通报重要事件。

SNMP 是一个应用层协议，是 TCP/IP 协议族的一部分，在 UDP、IP 及有关的特殊网络协议（如 Ethernet、FDDI、X.25）之上实现。

T

TACACS+

Terminal Access Controller Access Control System (TACASC) 认证协议，网络卫士安全网关支持的一种第三方认证机制，支持多个集中式数据库，适用于用户数量巨大的大型网络。TACASC 认证协议还提供授权 (Authorization) 和稽核 (Accounting) 服务。

TCP 协议

TCP (Transmission Control Protocol) 传输控制协议，该协议是为了在主机间实现高可靠性通信的包交换传输协议。TCP 是一种面向连接的端到端的可靠协议。

特殊对象

是一类用于描述网络访问控制相关资源的逻辑对象，网络卫士安全网关支持的特殊对象包括透明网络、文件资源、URL、关键字、邮件地址、用户认证数据库、用户、特殊端口、NAT 保留端口和多播组等。

通信策略

通信策略是一种描述防火墙如何修改数据包报文规则的策略，本版本支持 4 种通信策略：不做转换、源地址转换、目的地址转换、和双向地址转换。其中不做转换是缺省通信策略。

透明模式

网络卫士防火墙的一种工作模式，适用于所有区域均处于同一网段的情况，在透明模式下，防火墙对接收的数据包不作任何改动（包括 IP 和 MAC 地址），直接转发。这模式下，除了内网接口，其他接口均可以不设置 IP 地址。设置内网接口的 IP 地址是为了方便用户通过集中管理器管理防火墙。

Tear Drop

一种 DoS 攻击，利用的是系统在实现时的一个错误，重新设置 IP 包头的偏移量，造成数据报组装时的负数长度，导致系统崩溃。

U

UDP 协议

UDP（User Datagram Protocol）用户数据报协议，定义了互连网络环境中提供包交换的计算机通信的协议。

V

VieCA

网络卫士安全网关支持的一种第三方认证机制，主要是通过用户的计算机硬件信息对用户进行身份认证。基本机制是首先用户需要在离线状态下从管理员那里获得一个 VieCA 注册码，然后用户可以通过这个注册码登录 VieCA 服务器进行注册。在注册过程中，VieCA 服务器会收集用户所使用计算机的硬件信息。在以后的认证过程中，VieCA 会把试图登录防火墙的用户的计算机硬件信息与存储于服务器内的信息进行对比，从而确定用户身份。这种认证方式的过程中不涉及用户私人信息的交换，但是，它的安全性依赖于对用户计算机的访问控制措施是否完善。

VPN

即虚拟专用网（Virtual Private Network），定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过非安全网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展，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。VPN 主要技术包括隧道技术与安全技术。

VLAN

即虚拟局域网技术（Virtual Local Area Network），是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的新兴技术。目前 VLAN 技术标准主要有 IEEE 的 802.1Q 协议和 ISL 协议。VLAN 的实现方法主要有：静态和动态。静态 VLAN 是明确设定交换机端口属于哪个 VLAN 的方法，也称为基于端口的 VLAN。本版本仅支持静态 VLAN 技术。

VRC 认证

网络卫士安全网关支持的一种第三方认证机制，采用标准 CA 认证方式对用户进行认证。合法用户可以通过申请来获得一个 CA 所颁发的数字证书来证明自己的身份，数字证书包含有数字签名，用户私钥等信息。当进行身份验证时，通讯的另一方可以通过从 CA 获得的公钥，利用非对称算法来核对证书，从而确保用户的合法性。

W

网络对象

是用于描述网络设备或设备组对象的总称，网络卫士安全网关支持的网络对象包括节点、子网、对象组和负载均衡组。

WEB 重定向

是一项用于控制用户访问 Web 的技术。当用户试图登录访问某网站时，安全网关将自动的将用户转向其它 Web 服务器，如内部认证服务器，转向的网页可以是网站内的其它网页，也可以是其它网站。在确认用户已访问重定向网页后，安全网关会自动将用户访问请求转向原来访问的网页。

X

虚系统

所谓虚系统，就是在同一台设备的根系统上逻辑地划分出一套或多套相对独立的虚拟系统，每个虚拟系统都维护自己的配置，包括接口、对象、以及访问控制策略。

Y

用户

是一类网络卫士安全网关可自定义的特殊对象，表示正在或可能使用计算机系统或网络的人或进程。

用户认证数据库

网络卫士安全网关支持第三方认证协议，如 RADIUS 等。这些认证协议一般有一个服务器，存放着所有用户的信息。在有的环境中，同一个认证协议可以使用两个不同的服务器用于不同的目的，也可以多台相同服务器使用在一个环境中。网络卫士安全网关称这样的服务器为用户认证数据库。管理员可以在定义了认证数据库后，指定可以从某个防火区穿过安全网关到访问另一个防火区的用户，安全网关根据用户认证数据库中的信息来判断访问操作是否合法。

源地址转换策略

基本原理是在发送数据包时，把源 IP 地址转换为别的 IP 地址。同时目的主机将返回的数据包直接发送到转换后的 IP，当安全网关收到该数据包后，可以根据 NAT 映射表，修改该数据包的目的 IP 地址，并转发到对应 IP 主机。

网络卫士安全网关支持定义两种源地址转换策略：静态和动态。静态是指安全网关把所有符合该策略的数据包的源 IP 地址转换为该数据包转发接口的 IP 地址或某个指定 IP；动态转换则是首先需要定义一个地址池，当应用动态转换策略时，安全网关将把数据包的源地址动态地转换成为地址池中的某一地址。

Z

子网

表示一段连续的 IP 地址。

状态检测

状态检测是一种基于连接的状态检测机制，基于通过安全网关的数据包报头中收集相关信息，包括源地址、源端口、目的地址和目的端口等，在安全网关建立每个 TCP 会话或 UDP 伪会话的“状态”，也就是将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。当响应数据包到达时，安全网关将对比其报头中报告的信息和检查表中存储的相关会话的状态，当数据包状态成功匹配，防火墙将允许该数据包通过，否则丢弃。与包过滤不同，状态检测防火墙包含了通信信息和通信状态的匹配。

状态同步协议 SSP

是由天融信公司自行制定的，在负载均衡或双机热备工作方式下防火墙状态信息同步协议。网络卫士防火墙建议在负载均衡和双机热备工作方式下选择打开状态同步协议，这样当一台防火墙出现故障时，故障端口的通信不需要重新建立，备份墙或另一台防火墙就可以接替故障防火墙继续工作，对于网络用户是透明的。

阻断规则

是一种根据数据包的来源和数据包的特征，对非法入侵数据进行细粒度的分析和过滤的防火墙安全策略，可以更好地保证网络的安全性。与防火墙上设置访问策略相比，数据包过滤特征有所不同，粒度更细。

声明：

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。
2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。
3. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。
4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。