

声明

服务修订：

- 本公司保留不预先通知客户而修改本文档所含内容的权利。

有限责任：

- 本公司仅就产品信息预先说明的范围承担责任，除此以外，无论明示或默示，不作其它任何担保，包括（但不限于）本手册中推荐使用产品的适用性和安全性、产品的适销性和适合某特定用途的担保。
- 本公司对于您的使用或不能使用本产品而发生的任何损害不负任何赔偿责任，包括（但不限于）直接的、间接的、附加的个人损害或商业损失或任何其它损失。

版权信息：

- 任何组织和个人对本公司产品的拥有、使用以及复制都必须经过本公司书面的有效授权。

网御神州科技（北京）有限公司

目 录

1. 导 言	9
1.1. 本书适用对象	9
1.2. 手册章节组织	9
1.3. 菜单结构说明	11
1.4. 相关参考手册	16
2. 登录安全网关 WEB 界面	18
2.1. 管理员必读	18
2.1.1. 管理员电子钥匙	18
2.1.2. 管理员证书	19
2.1.3. 管理员配置管理	19
2.2. 管理员首次登录	20
2.2.1. 登录 WEB 界面	21
2.2.2. 登录命令行界面	24
2.3. 管理员再次登录	24
3. 首 页	26
4. 系统配置	29
4.1. 系统配置>>系统时钟	29

4.2. 系统配置>>升级许可.....	31
4.3. 系统配置>>导入导出.....	32
4.4. 系统配置>>报警邮箱.....	33
4.5. 系统配置>>日志服务器.....	34
4.6. 系统配置>>域名服务器.....	35
5. 管理配置.....	37
5.1. 管理配置>>管理方式.....	37
5.2. 管理配置>>管理主机.....	38
5.3. 管理配置>>管理员帐号.....	39
5.4. 管理配置>>管理员证书.....	43
5.5. 管理配置>>集中管理.....	45
6. 网络配置.....	48
6.1. 网络配置>>网络接口.....	48
6.2. 网络配置>>接口 IP.....	52
6.3. 网络配置>>策略路由.....	56
6.4. 网络配置>>静态 ARP.....	60
6.5. 网络配置>>DHCP 配置.....	61
6.5.1. DHCP 配置>>DHCP 服务器.....	62
6.5.2. DHCP 配置>>DHCP 中继.....	65

7. VPN 配置	67
7.1. 基本配置	68
7.2. VPN 客户端分组	70
7.3. VPN 端点	73
7.4. VPN 隧道	80
7.5. VPN 策略	84
7.6. 证书管理	87
7.6.1. 证书管理>>CA 证书	87
7.6.2. 证书管理>>对方证书	88
7.6.3. 证书管理>>本地证书	91
7.6.4. 证书管理>>证书吊销列表.....	94
8. 对象定义	96
8.1. 对象定义通用功能介绍.....	96
8.1.1. 分页显示.....	97
8.1.2. 查找	98
8.1.3. 排序	99
8.1.4. 添加	99
8.1.5. 编辑（修改）	100
8.1.6. 删除	102
8.1.7. 名称和备注	103

8.2. 地址.....	103
8.2.1. 地址>>地址列表	104
8.2.2. 地址>>地址组	106
8.2.3. 地址>>服务器地址.....	107
8.2.4. 地址>>NAT 地址池	110
8.3. 服务.....	112
8.3.1. 服务>>服务列表	113
8.3.2. 服务>>服务组	119
8.4. 代理.....	120
8.4.1. 代理>>预定义代理.....	121
8.4.2. 代理>>自定义代理.....	126
8.5. 时间.....	126
8.5.1. 时间>>时间列表	127
8.5.2. 时间>>时间组	129
8.6. 带宽列表	130
8.7. URL 列表.....	132
9. 安全策略.....	135
9.1. 安全策略>>安全规则.....	135
9.1.1. 包过滤规则	142
9.1.2. NAT 规则	146

9.1.3. IP 映射规则	151
9.1.4. 端口映射规则	155
9.1.5. 代理规则.....	161
9.2. 安全策略>>地址绑定.....	164
9.3. 安全策略>>IDS 联动.....	171
9.4. 安全策略>>抗攻击	174
9.5. 安全策略>>P2P 限制	185
9.6. 安全策略>>连接限制.....	188
9.6.1. 保护主机.....	188
9.6.2. 保护服务.....	190
9.6.3. 限制主机.....	193
9.6.4. 限制服务.....	195
10. 高可用性.....	198
10.1. 高可用性>>HA 基本参数.....	199
10.2. 高可用性>> HA 监控网口	204
10.3. 高可用性>> HA 监控 IP.....	205
11. 用户认证.....	209
11.1. 用户认证>>服务器	210
11.2. 用户认证>>用户列表.....	213
11.3. 用户认证>>用户组	217

12. 系统监控	222
12.1. HA 状态.....	223
12.2. 日志信息	224
12.3. 资源状态	227
12.4. 网络接口	229
12.5. VPN 隧道监控	231
12.6. DHCP 用户信息	232
12.7. 在线用户	233
12.8. 在线管理员.....	234
12.9. ARP 表.....	234
12.10. IP 诊断.....	235
附录一 用户认证客户端软件安装使用指南	237
1.概述.....	237
2.客户端软件的安装.....	238
3.基本使用方法	238
3.1 客户端主界面	238
3.2 配置系统	239
3.3 认证.....	239
3.4 修改密码	241
4.电子钥匙的使用方法	242

4.1 电子钥匙驱动程序的安装	242
4.2 配置电子钥匙	243
4.3 修改电子钥匙 PIN 口令	244
4.4 认证	245
4.5 修改口令	247

1. 导 言

1.1. 本书适用对象

本手册是 SecGate 3600-G10 安全网关管理员手册中的一本，主要介绍如何通过 WEB 页面方式对 SecGate 3600-G10 安全网关进行配置管理。

本手册适用于负责支持、维护 SecGate 3600-G10 安全网关的安全管理员，是对 SecGate 3600-G10 安全网关进行配置管理时的必备手册。

使用本手册的读者，应首先掌握 TCP/IP 协议、IP 地址及子网掩码等基本知识。

1.2. 手册章节组织

本手册按以下的章节编排：

第一章、引言：描述本书适用的读者，手册章节组织、WEB 界面菜单结构及相关参考手册等。

第二章、快速入门：描述了 SecGate 3600-G10 安全网关管理员首次登录方法和必读的基本知识。

第三章、首页：介绍了 SecGate 3600-G10 安全网关首页的显示信息及基本操作。

第四章、系统配置：介绍了 SecGate 3600-G10 安全网关相关的系统配置，包括：

系统时钟、升级许可、导入导出、报警邮箱、日志服务器、域名服务器等。

第五章、管理配置：讲述与SecGate 3600-G10安全网关管理相关的配置，包括：管理方式、管理主机、管理员帐号、管理员证书、集中管理等。

第六章、网络配置：介绍与网络环境相关的配置，包括：网络接口、接口IP、策略路由、静态ARP、DHCP服务器、DHCP中继等。

第七章、VPN配置：讲述VPN的相关配置，包括：VPN基本配置，VPN客户端分组、VPN端点，VPN隧道、VPN策略、证书管理等。

第八章、对象定义：讲述各种对象的定义方法，这些对象可供安全规则使用，包括：地址列表、地址组、服务器地址、NAT地址池，服务列表、服务组、预定义代理、自定义代理、时间列表、时间组、带宽列表、URL列表等。

第九章、安全策略：介绍与访问控制相关的配置，包括：安全规则、地址绑定、IDS联动、抗攻击、P2P限制、连接限制等。

第十章、高可用性：介绍 HA 的相关配置，包括：HA 基本参数、HA 监控网口、HA 监控 IP。

第十一章、用户认证：介绍与用户认证相关的设置，包括：服务器、用户列表、用户组。

第十二章、系统监控：介绍如何监控系统的运行状态，包括：HA 监控、日志信息、资源状态、网络接口、VPN 隧道监控、DHCP 用户信息、在线用户、在线管理员、ARP 表、IP 诊断等。


附录一：介绍了用户认证客户端软件的安装和使用。

1.3. 菜单结构说明

界面框架如下图所示：



















菜单采用树型结构，如下图所示：

一级菜单	说明
首页  首页	显示安全网关基本信息、网口接口状态、资源状态、在线管理员、最近事件等
系统配置	安全网关的系统配置，包括：

	<ol style="list-style-type: none"> 1) 系统时钟 2) 升级许可 3) 导入导出 4) 报警邮箱 5) 日志服务器 6) 域名服务器
<p>管理配置</p> 	<p>安全网关的管理配置，包括：</p> <ol style="list-style-type: none"> 1) 管理方式 2) 管理主机 3) 管理员帐号 4) 管理员证书 5) 集中管理 <p>其中，只有超级管理员 admin 才能修改管理员的帐号。</p>
<p>网络配置</p>	<p>安全网关作为一台网络设备，对网络相关属性的配置：</p> <ol style="list-style-type: none"> 1) 网络接口 2) 接口 IP 3) 策略路由 4) 静态 ARP 5) DHCP 配置：DHCP 服务器，DHCP 中继

<ul style="list-style-type: none"> ▼ 网络配置  网络接口  接口IP  策略路由  静态ARP ▼ DHCP配置  DHCP服务器  DHCP中继 	
<p>VPN 配置</p> <ul style="list-style-type: none"> ▼ VPN 配置  基本配置  VPN 客户端分组  VPN 端点  VPN 隧道  VPN 策略 ▼ 证书管理  CA证书  对方证书  本地证书  证书吊销列表 	<ol style="list-style-type: none"> 1) 基本配置 2) VPN 客户端分组 3) VPN 端点 4) VPN 隧道 5) VPN 策略 6) 证书管理：CA 证书，对方证书，本地证书，证书吊销列表
<p>对象定义</p>	<p>为简化安全网关安全规则的维护工作，引入了对象定义，可以定义如下对象：</p>

<ul style="list-style-type: none">▼ 对象定义<ul style="list-style-type: none">▼ 地址<ul style="list-style-type: none"> 地址列表 地址组 服务器地址 NAT地址池▼ 服务<ul style="list-style-type: none"> 服务列表 服务组▼ 代理<ul style="list-style-type: none"> 预定义代理 自定义代理▼ 时间<ul style="list-style-type: none"> 时间列表 时间组▼ 连接限制<ul style="list-style-type: none"> 保护主机 保护服务 限制主机 限制服务 带宽列表 URL列表	<p>1) 地址：地址列表、地址组、服务器地址、NAT 地址池</p> <p>2) 服务：服务列表、服务组</p> <p>3) 代理：预定义的 HTTP、FTP、TELNET、SMTP、POP3 代理、自定义代理</p> <p>4) 时间：时间列表、时间组，可以设置一次性调度和周循环调度</p> <p>5) 带宽列表：设置一些带宽属性</p> <p>6) URL 列表：黑白 URL 名单</p> <p>对象只有被安全规则引用才能起作用，否则，不起作用。策略管理员具有定义对象的权限。</p>
--	---

<p>安全策略</p> <ul style="list-style-type: none"> ▼ 安全策略 SEC 安全规则 SEC 地址绑定 SEC IDS联动 SEC 抗攻击 SEC P2P限制 ▼ 连接限制 SEC 保护主机 SEC 保护服务 SEC 限制主机 SEC 限制服务 	<p>安全网关的核心配置，包括：</p> <ol style="list-style-type: none"> 1) 安全规则：包过滤规则、NAT 规则、端口映射规则、IP 映射规则、代理规则。 2) 地址绑定：IP/MAC 地址的绑定 3) IDS 联动：设置与 IDS 产品之间的联动 4) 抗攻击：管理员可以针对不同的物理接口启用抗 Syn Flood 攻击、ICMP Flood 攻击、Ping of Death 攻击、UDP Flood 攻击、PING SWEEP 攻击、TCP 端口扫描、UDP 端口扫描、WinNuke 攻击。 5)P2P 限制:可以针对目前流行的 P2P 协议 apple、ares、bt、dc、edonkey、gnu、kazaa、soul、winmx 进行禁止使用、允许使用不做任何限制、允许使用且进行流量控制 6) 连接限制： 保护主机、保护服务、限制主机、限制服务
<p>高可用性</p> <ul style="list-style-type: none"> ▼ 高可用性 SEC HA基本参数 SEC HA监控网口 SEC HA监控IP 	<p>高可用性（High Availability，简称 HA）配置，包括：</p> <ol style="list-style-type: none"> 1) HA 基本参数 2) HA 监控网口 3) HA 监控 IP
<p>用户认证</p>	<p>用户认证包括：</p> <ol style="list-style-type: none"> 1) 用户认证服务器

<ul style="list-style-type: none"> ▼ 用户认证  服务器  用户列表  用户组 	<ul style="list-style-type: none"> 2) 用户列表 3) 用户组
<p>系统监控</p> <ul style="list-style-type: none"> ▼ 系统监控  HA状态  日志信息  资源状态  网络接口  VPN隧道监控  DHCP用户信息  在线用户  在线管理员  ARP表  IP诊断 	<p>监控安全网关所在网络以及安全网关本身的状态，包括：</p> <ul style="list-style-type: none"> 1) HA 状态： 2) 日志信息 3) 资源状态：CPU 利用率、内存利用率 4) 网络接口 5) VPN 隧道监控 6) DHCP 用户信息 7) 在线用户：当前通过用户认证功能的在线用户的信息 8) 在线管理员：显示所有在线管理的信息 9) ARP 表：系统内部 ARP 表的状态 10) IP 诊断：从安全网关 ping、traceroute 其它主机 <p>日志审计员具有监控安全网关所在网络以及安全网关本身的权限。</p>

1.4. 相关参考手册

《网御神州 SecGate 3600-G10 安全网关快速指南》，介绍了安全网关的快速安

装配置等。

《网御神州 SecGate 3600-G10 安全网关命令行操作手册》，介绍了如何通过命令行操作管理 SecGate 3600-G10 安全网关。

2. 登录安全网关 WEB 界面

2.1. 管理员必读

2.1.1. 管理员电子钥匙

管理员电子钥匙是默认的管理员身份认证方式，用于认证管理主机，确保与安全网关相连接的管理主机是合法的。

电子钥匙内保存了安全网关 ID、安全网关 IP 和端口，通过客户端软件读出，发给安全网关进行认证。认证通过后，安全网关（服务器端）为管理主机（客户端）IP 打开访问 https 公有证书的端口。每 5 秒钟安全网关进行一次通信监控。当安全网关检测到客户端退出(或者超时)，关闭管理主机访问 https 公有证书的端口的权限，并提供日志记录功能。

利用客户端软件可以修改电子钥匙中的安全网关 ID、安全网关 IP 地址和端口、电子钥匙访问口令 PIN。

随机光盘中提供一个电子钥匙的生产或修复程序：可以设置安全网关 ID，设置安全网关 IP 地址和端口，修改电子钥匙访问口令 PIN。

参考附录《用户认证客户端软件安装使用指南》中的第 4 节“电子钥匙的使用方法”。

2.1.2. 管理员证书

管理员可以用证书方式进行身份认证。证书包括 CA 证书、安全网关证书、安全网关私钥、管理员证书。前三项必须导入安全网关中，后一个同时要导入管理主机的 IE 中。

证书文件有两种编码格式：PEM 和 DER，后缀名可以有 pem，der，cer，crt 等多种，后缀名与编码格式没有必然联系。

CA 证书、安全网关证书和安全网关私钥只支持 PEM 编码格式，cacert.crt 和 cacert.pem 是完全相同的文件。管理员证书支持 PEM 和 DER 两种，因此提供 administrator.crt 和 administrator.der 证书，administrator.crt 和 administrator.pem 是完全相同的文件。*.p12 文件是将 CA、证书和私钥打包的文件。

2.1.3. 管理员配置管理

在管理主机上，通过电子钥匙认证或管理员证书认证成功后，再使用管理员帐号认证成功后才能访问安全网关可管理 IP，完成对安全网关的配置管理。请参考本手册中“管理配置”一章。

安全网关管理 IP 地址：管理员要在安全网关上定义安全网关可以被管理的 IP 地址，并指定管理主机可以进行的操作（如：允许 PING、允许 TRACEROUTE 等）。未指定为管理 IP 的主机不能管理。

安全网关带外管理口：MNG 口专门为管理设计，该网口上所有 IP 均可用作管理

IP。推荐用户使用带外管理口——MNG 口。MNG 口也可以与日志服务器连接。

管理主机地址限制：只有管理主机才能对安全网关进行管理。安全网关系统指定管理主机的 IP，最多可以指定 6 个管理主机，同时提供一个集中管理主机。

管理员身份认证方式：电子钥匙认证和证书认证。

管理员授权：管理员有不同的身份，分为超级管理员、配置管理员、审计管理员、策略管理员。其中，超级管理员可以增加、删除管理员帐号，不能直接配置管理；配置管理员可以设置系统配置、管理配置、网络配置；策略管理员可以配置对象定义、安全策略。审计管理员可以查看安全网关日志信息。

管理员访问信道加密：为防止管理员与安全网关之间的管理信息被非法者截取而利用，对安全网关的远程管理的通信应该实现加密。同时，安全网关可以防止对远程管理的重放攻击。CLI 界面命令行方式下支持 SSH 加密，WEB 界面下支持 SSL 加密（使用 https 协议访问安全网关）。通过安全网关本地串口使用超级终端登录时通信不加密。

2.2. 管理员首次登录

正确管理安全网关前，需要配置安全网关的管理主机、管理员帐号和权限、网口上可管理 IP、安全网关管理方式。

- 默认管理员帐号为 admin，密码为 firewall
- 默认管理口：带外管理口 MNG 口
- 可管理 IP：mng 口上的默认 IP 地址为 10.50.10.45/255.255.255.0

- 管理主机：默认为 10.50.10.44/255.255.255.0
- 默认管理方式：(1) 管理主机与 mng 网口连接，访问 <https://10.50.10.45:8888>，登录帐号为默认管理员帐号与密码，访问 WEB 界面。此方式下的配置通信是加密的。(2)管理主机 COM 串口与安全网关 CONSOLE 口连接，登录账号为默认管理员账号与密码，访问命令行界面。

2.2.1. 登录 WEB 界面

将默认管理主机的网口用交叉连接的以太网线(两端线序不同)与安全网关的 MNG 口连接，管理主机的 IE 版本必须是 5.5 及以上版本，在浏览器中输入 <https://10.50.10.45:8888>，如果是证书认证，则输入 <https://10.50.10.45:8889>，登录后弹出下面的登录界面：





正确输入默认管理员帐号（admin）与密码（firewall），进入下面的安全网关配置管理界面：



在第一次登录成功后，管理员可以按需求变更管理员帐号、管理主机、安全网关可管理 IP、管理方式或导入管理员证书。下次登录时，按变更内容进行认证与登录。

当管理员完成管理任务或者离开管理界面时，应主动退出 WEB 管理界面。正确

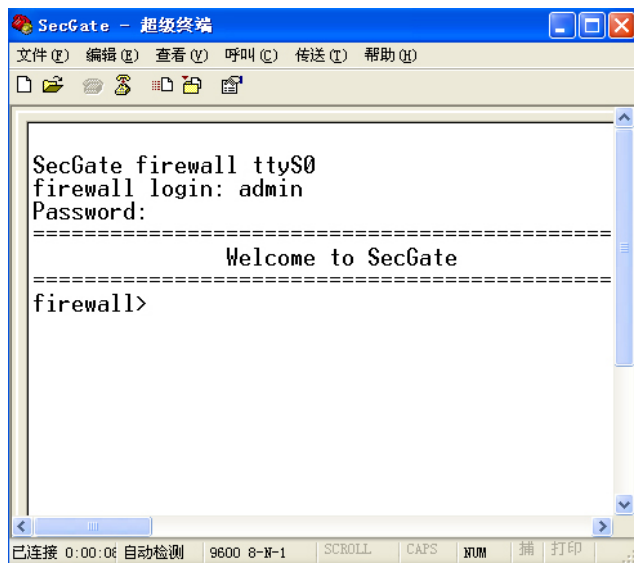
的操作方法是点击快捷菜单最右端的“退出”快捷图标 ，这将通知安全网

关本管理员退出操作，然后关闭本窗口。如果点击 IE 标题栏上的 ，则只是

关闭了窗口，并没有通知安全网关该管理员已退出管理。安全网关 WEB 界面有超时机制，默认超时时间为 600 秒，如果安全网关持续 (>600 秒) 未接收到 WEB 界面操作请求，则超时退出。

2.2.2. 登录命令行界面

将管理主机的 COM 串口与安全网关的 CONSOLE 口用串口线连接，配置管理主机的超级终端，波特率为 9600 比特。以默认管理员帐号与密码登录，进入 CLI 命令行界面：



在第一次登录成功后，管理员可以按需求变更管理员帐号、管理主机、安全网关可管理 IP，管理方式或导入管理员证书。下次登录时，按变更内容进行认证与登录。


2.3. 管理员再次登录

当管理主机与安全网关的通用网口连接，并为其配置可管理 IP，则管理员需要电子钥匙进行身份认证或者管理员证书方式认证。

- 管理员将与安全网关匹配的电子钥匙插入管理主机上，正确输入电子钥匙 PIN 码（初始 12345678）后，打开安全网关管理员身份认证程序。绿图标表示认证通过，红图标表示认证失败或未登录。认证成功后可以访问 <https://安全网关可管理 IP:8888>，在登录界面中输入管理员帐号与密码，进行安全网关配置管理界面。
- 使用管理员证书方式时，需要在安全网关上导入管理员证书，在管理主机上导入管理员证书，访问 <https://安全网关可管理 IP:8889>，认证成功后，进入安全网关配置管理界面。

具体说明请参考“管理员必读>>管理员配置管理”一节，具体操作过程请参考本手册中“管理配置”一章。

3. 首 页

首页集中扼要地显示了各种监控信息，点击[更多>>](#)将跳转到相应的界面，查看更详细的信息。在任何界面中，点击  [首页](#) 后，返回首页。

首页监控的信息主要包括：

- (1) 安全网关设备自身信息
- (2) 网络接口
- (3) 资源状态
- (4) 在线管理员
- (5) 最近事件


首页内容如下图所示：



首页信息说明：

域 名	说 明
<div style="background-color: #4f81bd; color: white; padding: 2px 5px; display: inline-block;"> ▣ 设备信息 </div>	设备信息区域显示安全网关的序列号、硬件版本号、软件版本号和网关名称。
<div style="background-color: #4f81bd; color: white; padding: 2px 5px; display: inline-block;"> ▣ 网络接口 </div>	网络接口区域显示安全网关的所有网络接口根据模块的不同，会有 FE1, FE2, FE3, FE4、FE5、FE6、FE7、FE8、GE1、GE2、GE3 的连接状态以及发送、接收的字节数。

 资源状态	资源状态区域显示了 CPU 和内存的利用率以及安全网关的连接数。
 在线管理员	在线管理员区域显示了所有的在线管理员的名称、登录方式、登录地点和登录时间。
 最近事件	最近事件区域显示了最近时间段的日志信息。
 保存配置	保存安全网关的当前配置。
 导出配置	导出安全网关保存过的配置。  导出配置之前，必须先保存配置。
 帮助信息	查看安全网关的 FAQ。
 退出	退出 WEB 界面。  当管理员完成管理任务或者离开管理界面时，应主动退出 WEB 管理界面。

 首页面会按照所设置的刷新时间定时自动进行刷新，如果管理员停留在首页面，并且所设置的刷新时间小于系统超时时间（默认为 600 秒），则该 WEB 界面永远不会超时退出。对于管理员来说，如果长时间离开 WEB 管理界面，为了杜绝管理上的安全漏洞，请务必不能停留在该界面上，必须执行退出操作。

4. 系统配置

4.1. 系统配置>>系统时钟

安全网关系统时间的准确性是非常重要的。因为安全网关的时间调度功能是以安全网关的系统时间为依据标准，时间调度是判断当前时间是否匹配规则中的时间段，从而决定是否可以访问某些功能，其中的当前时间正是此处设置的系统时钟。

SecGate 3600-G10 安全网关的系统时间可以设置为与管理主机的时间同步，也可以设置为与时钟服务器的时间同步。

安全网关的时间更新后，不需要系统保存或重启，会使用新调整的时间。

系统配置>>系统时钟

日期时间

安全网关当前时间:
 管理主机当前时间:

时钟服务器

启用时钟服务器
 时钟服务器 IP:
 每隔: 分钟同步一次 (范围: 1-85535 默认: 5 分钟)

系统时钟菜单说明:

域 名	说 明
-----	-----

<p>时间同步</p>	<p>与管理主机时间同步</p> <p>调整管理主机时钟，点击“时间同步”按钮，安全网关立即与管理主机时间同步。</p>
<p><input type="checkbox"/> 启用时钟服务器</p>	<p>启用与时钟服务器的时间同步功能</p> <p>启动后，安全网关的系统时钟与网络时钟服务器同步（支持 NTP 协议）</p> <p>同步方式有两种：（1）立即同步（2）周期性自动同步</p>
<p>时钟服务器 IP:</p>	<p>输入安全网关可以访问的时钟同步服务器的 IP 地址。</p>
<p>立即同步</p>	<p>与时钟服务器时间立即同步:</p> <p>选中“启用时钟服务器”，输入“时钟同步服务器 IP”，点击“立即同步”按钮，安全网关立即与时钟服务器时间同步。</p> <p>注意 点击“立即同步”按钮后，界面将在 60 秒内刷新。</p>
<p>每隔: <input type="text" value="5"/> 分钟同步一次</p>	<p>与时钟服务器时间周期性自动同步:</p> <p>选中“启用时钟服务器”，输入“时钟同步服务器 IP”，设定同步周期间隔时间，点击“确定”按钮，安全网关在指定时间与时钟服务器时间同步。</p>

注意 调整安全网关时间以后，有可能造成界面超时退出，因为判断是否超时用到了安全网关的当前时间。超时退出以后重新登录即可。

4.2. 系统配置>>升级许可

安全网关系统升级功能可以快速响应新的安全需求，保证安全网关的功能与安全的快速升级。安全网关的软件升级可以通过管理界面的模块升级方便进行，用户只需选择本地的安全网关升级包，点击升级后，重启安全网关即可完成升级功能。

系统配置>>升级许可

系统当前软件版本: 3.6.3.30

* 升级文件:

序号	升级以后版本号	更新描述	升级时间
2	3.6.3.30	BUILD TIME: Thu Mar 9 11:37:31 CST 2006	2006/03/09 11:37:31
1	3.6.6.22	AA	2006/12/12

升级菜单说明:

域 名	说 明
<input type="button" value="升级"/>	点击“浏览”按钮，选择管理主机上的升级包，点击“升级”按钮，点击“重启安全网关”按钮，重启安全网关，完成模块升级功能。
<input type="button" value="导出升级历史"/>	将升级历史导出到管理主机上做备份。
<input type="button" value="检查最新升级包"/>	管理员可以查看系统当前软件版本。点击“检查最新升级包”，系统会弹出新的 IE 窗口并连接安全服务网站，但要求安全网关可以连接 Internet。
<input type="button" value="重启安全网关"/>	点击“重启安全网关”按钮，安全网关将重新启动。



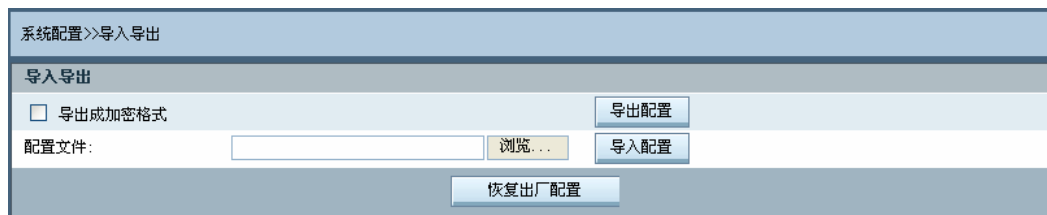
重启安全网关前，记住要保存当前配置。

4.3. 系统配置>>导入导出

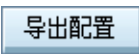

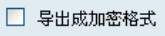
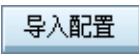
安全网关的导入导出功能便于管理员对配置信息进行备份，在需要的时候重新导入安全网关即可实时生效。




通过点击导出配置按钮，将当前的配置信息导出到管理主机上做备份。

也可以通过导入配置按钮将安全网关配置信息从管理主机上导入到安全网关上，重启安全网关后导入的配置信息立即生效。



导入导出菜单说明：

域 名	说 明
	点击“导出配置”按钮，安全网关当前的配置信息以文件的形式保存在安全网关系统外部。 配置文件的路径和名字由管理员指定。  选中  ，可以生成加密格式的配置文件。
	选择正确的配置文件，点“导入配置”，系统提示“安全网关

	系统重启，是否继续？”，选择“是”则系统重启，导入的配置信息生效；选择“否”，则“导入配置”操作失效。
	点击“恢复出厂配置”按钮，安全网关当前配置信息被系统删除，所有配置立即恢复到安全网关出厂时的配置。
	保存配置快捷键
	导出配置快捷键



导入配置后如果未重启安全网关，安全网关的所有功能和导入前一样正常工作，只有重启安全网关以后导入的配置才能生效。

4.4. 系统配置>>报警邮箱

设置安全网关的报警邮箱。在多次登录安全网关失败时、检测到对安全网关的恶意攻击时以及在 HA 功能切换时都向报警邮箱发送报警邮件。此功能有助于管理员对此类重要事件采取措施，及时响应。

系统配置>>报警邮箱


报警邮箱

* 报警邮箱:

SMTP服务器IP:

报警邮箱菜单说明：

域 名	说 明
-----	-----

报警邮箱	e-mail 地址。 以下情况将发送报警邮件：（1）管理员登录，两分钟内连续失败五次（2）网络监控报告（3）其它安全事件
测试邮箱	配置完成后，可点击按钮检查是否连通
确定	确定按钮指将配置生效
清空	清空按钮是清除上面输入的配置
	点击“修改 DNS 配置”按钮，转到“系统配置>>域名服务器”界面。如果不能正常发邮件，请检查 DNS 配置是否正确。

4.5. 系统配置>>日志服务器

安全网关各功能模块提供标准格式的日志记录。

启用日志记录的模块在有匹配此功能的数据包通过后，将记录日志，默认情况下日志存储在安全网关本地。此外也可以将日志信息直接发往日志服务器。

本菜单提供配置日志服务器的功能，将日志服务器与安全网关的网口相连，安全网关配置此服务器的 IP 地址和接收端口号（默认是 UDP 协议的 514 端口），即可将安全网关的所有模块日志发往此日志服务器，随机提供的日志服务器软件可以实现强大的存储和审计功能，方便管理员对日志进行查询和管理。

日志服务器

* 日志服务器 IP:

协议:

* 端口: (0-65535)

日志服务器菜单说明:

域 名	说 明
日志服务器 IP	日志服务器的 IP 地址
协议	安全网关与日志服务器通信的协议
端口	安全网关与日志服务器通信的端口
查看日志	点击“查看日志”按钮，转到“系统监控>>日志信息”界面



安全网关默认使用 syslog 方式向第三方发送日志，使用 UDP 协议的 514 端口。

4.6. 系统配置>>域名服务器

如果管理员设置了报警邮箱，则需要配置安全网关的域名服务器，用于安全网关自身向外发数据包时进行域名解析。

系统配置>>域名服务器

域名服务器

* 安全网关名称: (1-15位 字母、数字、减号、下划线的组合)

域名服务器1 IP:

域名服务器2 IP:

域名服务器菜单说明:

域 名	说 明
安全网关名称	安全网关主机名

域名服务器 1	配置域名服务器的 IP 地址，具有较高的优先级
域名服务器 2	配置域名服务器的 IP 地址，当第一个 DNS 服务器查不到时，会检查该 DNS 服务器。

5. 管理配置

5.1. 管理配置>>管理方式

安全网关默认提供 WEB 管理方式和 CLI 命令行管理方式，以及支持拨号（PPP）拨入方式管理安全网关。分别通过网口、串口和拨号(PPP)连接安全网关。上述三种管理方式是默认开启状态，管理员不能删除其中任一管理方式。

另外，安全网关还提供通过 SSH 对安全网关以命令行方式进行远程管理的功能，此管理方式管理员有权进行添加和删除。

管理方式	
<input checked="" type="checkbox"/>	超级终端管理（连接CONSOLE口）
<input checked="" type="checkbox"/>	支持拨号（PPP）接入（连接AUX口）
<input checked="" type="checkbox"/>	Web（https）管理
<input type="checkbox"/>	远程 SSH 管理
<input type="button" value="确定"/>	

管理方式菜单说明：

域 名	说 明
超级终端管理（连接 CONSOLE）	默认启用“超级终端”管理。管理主机 COM 串口与安全网关 CONSOLE 口连接，通过管理主机超级终端登录安全网关。使用默认管理员帐号和密码。
支持拨号（PPP）	默认启用“拨号(PPP)接入”，将管理主机 COM 串口与 modem1

接入（连接 AUX 口）	连接，安全网关的 AUX 口与 modem2 连接，modem1 与 modem2 间是通过电话线连通。从管理主机向安全网关拨号，拨号成功后，安全网关与管理主机建立了 PPP 连接。
WEB（https）管理	默认启用“WEB（https）管理” 管理主机可以通过网口上的管理 IP 登录安全网关 WEB 界面，需要电子钥匙或管理员证书认证。
远程 SSH 管理	启用“远程 SSH 管理”，管理主机通过网络可连接到安全网关网口（有可管理 IP）时，以 SSH 方式（如：利用 putty 软件等）登录安全网关命令行界面。

5.2. 管理配置>>管理主机

管理员要想管理安全网关，必须增加管理主机，即通过此菜单添加管理主机的 IP，然后通过网口连接安全网关即可进行管理。安全网关最多支持 256 个管理主机对其进行管理。

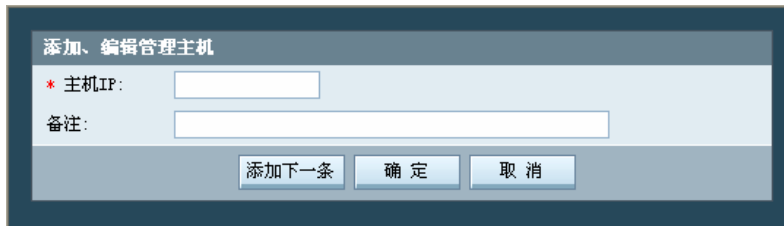
管理配置>>管理主机		集中管理	请输入关键字	查找
序号	管理主机IP	备注	操作	
1	10.50.10.44	出厂默认管理主机	 	
<input type="button" value="添加"/>				
首页 上一页 下一页 尾页				
第1页/1页 跳转到 <input type="text" value="1"/> 页 <input type="button" value="确定"/>				
每页 <input type="text" value="全部"/> 行				

管理主机菜单说明：

域 名	说 明
-----	-----

管理主机 IP	管理员只有在管理主机上才能对安全网关进行管理。 最多支持 256 个管理主机 IP 和 1 个集中管理主机。
操作	添加、编辑、删除管理主机 IP

在“管理主机”界面点击 ，弹出以下界面



添加、编辑管理主机

* 主机IP:

备注:

域 名	说 明
主机 IP	管理主机的 IP 地址
备注	管理主机的说明信息，不能超过 255 个字符

5.3. 管理配置>>管理员帐号

安全网关支持多种管理员权限的帐号对其进行管理，分别为超级管理员、策略管理员和日志审计管理员。不同权限的用户只能在自己的权限范围内管理安全网关。通过此菜单可以灵活添加多个不同级别的帐号。

管理配置>>管理员帐号

允许多个管理员同时管理

帐号	帐号类型	操作
admin	超级管理员+配置管理员+策略管理员+日志审计员	

允许 (30 - 86400)秒内最多登陆失败次数为: (3 - 10)次

最后一次登陆失败后禁止: (30 - 86400)秒

管理员帐号菜单说明:

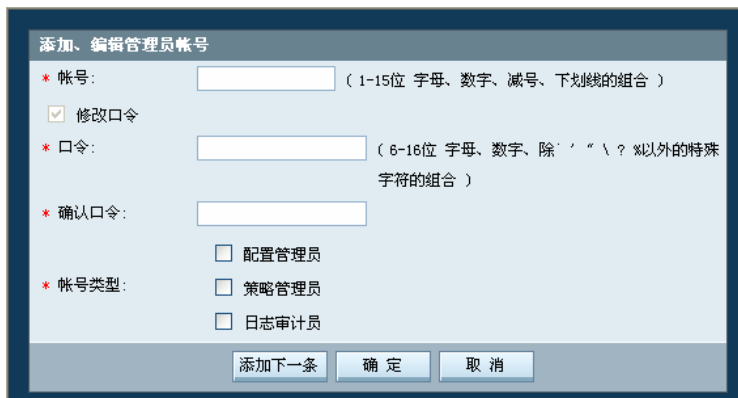
域 名	说 明
允许或禁止多个管理员同时管理	<p>选择“允许多个管理员同时管理”时，安全网关系统才会允许多个管理员同时登录。未选中“允许多个管理员同时管理”，如果此管理员访问非正常退出，在超时时间未到的情况下（超时时间默认为 10 分钟），该管理员如果使用另外的 IP 或帐号登录，则受超时时间限制，不能登录。但是如果此管理员仍使用相同的 IP 和帐号登录是可以的，不受超时时间限制。或者通过超级终端方式登录安全网关，利用管理员命令设置为“允许多个管理员同时管理”并登录。</p> <p>建议设置不允许多个管理员同时登录修改配置。</p> <p>默认只能有一个管理员登录安全网关进行配置管理。</p>
帐号	<p>管理员帐号。超级管理员可以添加多个授权不同的管理员帐号</p>

帐号类型	参考附表：管理员按级别授权管理说明
操作	添加、编辑、删除管理员帐号

附表：管理员按级别授权管理

管理员级别	授 权	备 注
超级管理员	增加、删除管理员帐号，不能直接配置管理	默认管理员帐号与密码为 admin: firewall。 帐号 admin 不能删除。
配置管理员	配置系统配置、管理配置、网络配置、VPN 配置、高可用性、用户认证	无默认帐号
策略管理员	配置对象定义、安全策略	无默认帐号
审计管理员	进行系统监控	无默认帐号

在“管理配置>>管理员帐号”，点击 **添加**，将弹出以下界面：



添加、编辑管理员帐号

* 帐号： (1-15位 字母、数字、减号、下划线的组合)

修改口令

* 口令： (8-16位 字母、数字、除 ' " \ ? % 以外的特殊字符的组合)

* 确认口令：

* 帐号类型： 配置管理员
 策略管理员
 日志审计员

域 名	说 明
-----	-----

帐号	管理员帐号
口令	管理员口令
确认口令	管理员口令，重复输入上一次的口令。
配置管理员	管理员权限。 可以配置系统配置、管理配置、网络配置、VPN 配置、高可用性、用户认证
策略管理员	管理员权限 可以配置对象定义、安全策略。
审计管理员	管理员权限 可以进行系统监控

备注：如果忘记了超级管理员的帐号，可以通过超级终端接入安全网关，使用系统恢复帐号：**rescue**，口令：**rescue** 来设置超级管理员的帐号和口令，该恢复帐号只能通过超级终端使用，并且其功能只是设置超级管理员，此外不再有其它功能。然后通过所设置的超级管理员管理安全网关。

在管理员帐号界面下为配置登陆策略

允许 (30 - 86400)秒内最多登陆失败次数为： (3 - 10)次

最后一次登陆失败后禁止： (30 - 86400)秒

默认配置为允许 120 秒内最多登陆失败次数为 5 次，当 5 次失败后，禁止 30 秒内再次登陆。具体时间参数可以由管理员来进行指定。

5.4. 管理配置>>管理员证书

本界面主要完成证书的管理。管理证书为标准的 CA 证书。

无论使用电子钥匙认证，还是直接使用证书认证，均是通过 **https** 协议访问，即为：使用管理证书完成 **SSL** 的加密。

管理员通过电子钥匙认证成功，访问 **https://安全网关可管理 IP:8888**，登录安全网关配置界面，使用安全网关 **WEB** 服务器的服务器端的证书进行信道加密。安全网关出厂时预置了一套证书（CA 中心证书、安全网关证书、安全网关密钥），管理员可以点击网御神州 CA 中心证书的链接、安全网关证书的链接进行查看。管理员也可以更新此套证书，按“管理配置>>管理员证书”界面提示直接导入即可。

管理员通过 **IE** 完成证书认证，访问 **https://安全网关可管理 IP:8889**，登录安全网关配置界面，使用安全网关 **WEB** 服务器的客户端的证书进行信道加密。当管理员使用证书方式进行身份认证时，必须在安全网关中导入一套证书（CA 中心证书、安全网关证书、安全网关密钥、管理员证书），并在管理主机的 **IE** 中导入管理员证书。管理员可以点击网御神州 CA 中心证书的链接、安全网关证书的链接进行查看。管理员可以查看导入的管理员证书列表。

管理配置>>管理员证书

SecGate CA中心

CA中心证书: 浏览...

安全网关证书: 浏览...

安全网关密钥: 浏览...

导入

* 管理员证书: 浏览...

导入

管理员证书列表:

生效	文件名	证书信息	操作
<input checked="" type="checkbox"/>	administrator.pem	颁发者 : SecGateCA 颁发给 : SecGateAdmin 有效期 : GMT 2006/02/13 10:09:15 - GMT 2016/02/11 10:09:15	

生效

此界面包括以下功能:

1. 到网御神州 CA 中心下载证书
2. 导入一套证书 (CA 中心证书、安全网关证书、安全网关密钥、管理员证书)
3. 查看 CA 中心证书、安全网关证书
4. 管理员证书维护 (生效、删除)

通过管理员证书管理安全网关的操作步骤:

1. 管理员向 CA 中心申请证书, 选择一套匹配的 CA 中心证书、安全网关证书、安全网关密钥“导入”。
2. 管理员要将选择匹配的管理员证书“导入”。点击“生效”, 使用相关管理员证书生效。
3. 下次登录安全网关系统前, 请将有效管理员证书导入管理主机的 IE 浏览器中,

访问 <https://安全网关可管理 IP:8889>，进入安全网关配置管理界面。

域 名	说 明
网 御 神 州 CA 中心	点击“网御神州 CA 中心”按钮，打开 CA 中心的主页，可以下载证书。
导入证书	CA 中心证书、安全网关证书、安全网关密钥的导入。 CA 中心证书、安全网关证书、安全网关密钥必须是配套的，且只接受 PEM 格式的证书 CA 中心证书、安全网关证书、安全网关密钥必须同时更换。
导入证书	管理员证书的导入。 管理员证书必须与导入的 CA 中心证书、安全网关证书、安全网关密钥完全匹配。
管 理 员 证 书列表	管理员证书列表包括生效和删除 在“生效”一栏选择要生效的证书，点击“生效”按钮则生效选中的证书。在“操作”一栏中，点击“删除”的图标，即删除此证书。

5.5. 管理配置>>集中管理

SecGate 3600-G10 安全网关通过 SNMPv2/v3 协议，实现了和网御神州集中安全管理系统的无缝集成，通过在安全网关上配置集中管理主机的 IP 地址，可以实现对安全网关的集中管理。

管理员配置集中管理主机的 IP 和各项监控信息的阈值。当安全网关运行信息超过

阈值后，通过 SNMP 协议与该集中管理主机发送 trap 信息。

监控信息包括 系统名字、版本号、序列号、CPU 利用率、内存利用率、网络接口状态、网络连通状态。通过 trap 信息发给集中管理中心，为网络管理人员提供全面、易用、高效的实时监控网络资源使用状况的工具和手段。相关信息也可以在安全网关的“系统监控>>网络接口”界面和“系统监控>>资源状态”查看。

管理配置>>集中管理

集中管理

启用集中管理: (启用时, 请您在安全规则中添加"允许集中管理主机访问安全网关secgate_global服务"的包过滤规则)

启用蜂鸣器报警:

集中管理主机 IP:

>>
<<

安全网关名称:

*CPU 利用率阈值: % (1-100之间的整数)

*内存利用率阈值: % (1-100之间的整数)

*文件系统利用率阈值: % (1-100之间的整数)

只读团体字符串: (32个以内字符)

读写团体字符串: (32个以内字符)

Trap发送字符串: (32个以内字符)

负责人姓名:

负责人电话:

本机备注:

集中管理菜单说明:

域 名	说 明
安全网关名称	本台安全网关名称
启用集中管理	是否启用集中管理的功能

启用蜂鸣器报警	安全网关开启蜂鸣器报警功能
集中管理主机 IP	集中管理主机 IP
CPU 利用率阈值	如果实际利用率超过该值, 则向集中管理主机发送报警信息
内存利用率阈值	如果实际利用率超过该值, 则向集中管理主机发送报警信息
文件系统利用率阈值	如果实际利用率超过该值, 则向集中管理主机发送报警信息
只读团体字符串	集中管理获取设备信息的密码
读写团体字符串	集中管理获取和设置设备信息的密码
Trap 发送字符串	陷阱管理器的密码
负责人姓名	本台安全网关负责人姓名
负责人电话	本台安全网关负责人电话
本机备注	对本台安全网关的描述



(1) 启用时, 请您在安全规则中添加"允许集中管理主机访问安全网关 secgate_global 服务"的包过滤规则, 集中管理主机才能和安全网关通信。

(2) 集中管理主机只能接收 trap 信息等, 并不能作为管理主机。如果需要集中管理主机同时也能管理安全网关, 则必须在“管理配置>>管理主机”中添加集中管理主机的 IP 地址。

6. 网络配置

此部分主要对安全网关的网络接口属性、安全网关 IP 地址和策略路由进行配置，是安全网关其他功能和安全规则配置的基础。





6.1. 网络配置>>网络接口

SecGate 3600-G10 安全网关通过配置网络接口（FE1-FE8、GE1、GE2、GE3）的属性信息，可提高安全网关系统的效率与安全性，保证对数据流的走向进行灵活、严格的控制。


网络配置>>网络接口								
接口名称	工作模式	MTU	网口速率	TRUNK	VLANID	非IP协议	日志	操作
fe1	路由	1500	自动协商	✘		✘	✘	
fe2	路由	1500	自动协商	✘		✘	✘	
fe3	路由	1500	自动协商	✘		✘	✘	
fe4	路由	1500	自动协商	✘		✘	✘	
fe5	路由	1500	自动协商	✘		✘	✘	
fe6	路由	1500	自动协商	✘		✘	✘	
fe7	路由	1500	自动协商	✘		✘	✘	
fe8	路由	1500	自动协商	✘		✘	✘	
ge1	路由	1500	自动协商	✘		✘	✘	
ge2	路由	1500	自动协商	✘		✘	✘	
ge3	路由	1500	自动协商	✘		✘	✘	

网络接口菜单说明：

域 名	说 明
接口名称	当前可用的网络接口，不可修改。其中，FE1—FE8 是 8 个百兆网络接口。GE1—GE3 是 3 个千兆 GBIC 接口。根据型号不同也会有 4 个千兆接口。
工作模式	路由或混合 路由模式指网口工作在纯路由方式下，非透明模式。 混合模式指网口工作在桥和路由的混合方式下，可实现透明模式工作及路由模式工作。
MTU	允许通过的 MTU 大小，可以设置为 256-1500。  如果主机发出的 TCP/UDP 报文打上了 DF（禁止分片）标记，则大于 MTU 的包将被安全网关抛弃。可以使用抓包工具（如：Ethereal 软件等）来辅助判断分析该现象。
网口速率	可以自动协商，也可以设置网口的速率，可选 10/100/1000M 全双工/半双工。
TRUNK	是否支持 trunk
VLAN	 表示允许，允许时可以接收 VLAN 数据包。  表示禁止，禁止时不能接收带 VLAN 标记的数据包。
VLANID	显示添加的 VLAN ID 号
非 IP 协议	 表示该网口允许接收到的非 IP 协议的数据包穿过。

	 表示该网口禁止接收到的非 IP 协议的数据包穿过。
日志	 表示该网口对接收数据包的安全过滤功能进行日志记录，主要针对非安全规则的过滤功能进行日志记录，如 IP/MAC 绑定、抗攻击等。  表示该网口不记录相关日志。
操作	 编辑：可以编辑各网口上启用的功能

编辑网口启用功能

列表中显示系统中全部的网口和各网口上启用的功能。点击“操作”一栏中的“编辑”图标，选择某个网口进行编辑，可以修改网口配置。如下图所示：

编辑网络接口信息

名称： (不能修改)

MAC 地址： (不能修改)

网口速率： ▼

工作模式： 路由模式 混合模式

* MTU： (256-1500)

支持TRUNK： VLAN ID (1-4094, 多个用英文逗号分隔)
 所有VLAN ID

非IP协议数据包： ▼

日志记录：

域 名	说 明
名称	<p>显示当前可用的网络接口，不可修改。</p> <p>其中 FE1—FE8 是 8 个百兆网络接口。GE1—GE3 是 3 个千兆网络接口。根据型号不同也会有 4 个千兆接口。</p>
MAC 地址	该网口的 MAC 地址，不可修改。
网口速率	可以设置网口速率，百兆可以设置为 10M/100M 全双工/半双工，千兆接口可以设置 1000M 全双工/半双工
工作模式	<p>路由模式指网口工作在纯路由方式下，非透明模式。</p> <p>混合模式指网口工作在桥和路由的混合方式下，可实现透明模式工作及路由模式工作。</p>
MTU	设置安全网关允许通过的 MTU 大小，可以设置为 256-1500。
支持 TRUNK	<p>启用该功能后，可以接收 VLAN 数据包。此时，安全网关该网口要与网络设备的 trunk 口连接。</p> <p>当管理员指定 VLAN ID 号时，安全网关在该网口只接收指定 ID 的 VLAN 数据包。</p> <p>当管理员选择支持 trunk 时，安全网关允许 trunk 中带 VLAN tag 的 VLAN 数据包和不带 VLAN tag 的裸数据包通过。</p>
非 IP 协议数据包	<p>对非 IP 协议的数据帧：在路由模式下禁止非 IP 协议数据包通过，在混合模式下按网口处配置的非 IP 协议过滤策略（允许或禁止）</p>

	执行，不检查安全规则。
日志记录	启用该功能后，可以对该网口接收数据包的安全过滤功能进行日志记录，主要针对非安全规则的过滤功能进行日志记录，如 IP/MAC 绑定、抗攻击等。




6.2. 网络配置>>接口 IP

- 提供 8 个百兆网口：8 个 10/100M 自适应以太网接口（FE1—FE8）
- 提供 3 个千兆网口：3 个 1000M 千兆接口（GE1—GE3）
- 提供 1 个虚网口设备 br：如果某些网口设置为混合方式，系统就会自动生成一个虚网口设备 br，并将这些混合模式的网口绑定在该虚网口设备上。即虚网口设备 br 可以看做是一个网口设备。

网络配置>>接口IP							
网络接口	接口IP	掩码	允许所有主机 PING	用于管理	允许管理主机 PING	允许管理主机 Traceroute	操作
mng	10.50.10.45	255.255.255.0	✘	✔	✔	✔	 
				<input type="button" value="添加"/>	<input type="button" value="刷新"/>		
首页 上一页 下一页 尾页		第1页/1页		跳转到 <input type="text" value="1"/> 页 <input type="button" value="确定"/>	每页 <input type="text" value="全部"/> 行 		

安全网关 IP 菜单说明：

域 名	说 明
网络接口	只显示配置了 IP 地址的网络接口，可能包括：FE1—FE8，GE1、GE2、GE3、GE4，虚网口设备“br”
安全网关 IP	显示配置在网口的安全网关 IP。同一个物理网口配置多个 IP 地址时显

	<p>示多条信息。</p> <p>设置为混合模式的物理网口属于虚网口设备 br，原配置的 IP 地址将由 br 这个虚设备使用。br 也可以无 IP 地址。</p> <p>注意 不同物理网口设备上不能设置相同网段的 IP 地址。</p>
掩码	安全网关 IP 地址的掩码
允许所有主机 PING	此项设置为允许后，则任何主机都可以 ping 安全网关该网口上的该 IP 地址。
用于管理	指定用于管理后，管理主机可以通过该 IP 地址对安全网关进行管理。
允许管理主机 PING	此项设置为允许，允许所有主机 PING 设置为不允许，管理主机可以 ping 安全网关该网口上的该 IP 地址，不是管理主机的则不能 ping 安全网关。
允许管理主机 Traceroute	此项设置为允许后，只允许管理主机执行 Traceroute，探测安全网关该网口上的该 IP 地址。
操作	可以添加  、编辑  、删除  相关的安全网关 IP 地址。

在“网络配置>>接口 IP”，点击 ，将弹出以下界面：

添加、编辑接口IP

* 网络接口:

* 接口IP:


* 掩码:

允许所有主机PING:

用于管理:

允许管理主机PING:

允许管理主机Traceroute:

域 名	说 明
网络接口	<p>设置为路由方式的网口，该界面显示的“网络接口”为物理网口的设备名，包括：FE1—FE8、GE1—GE3。安全网关 IP 配置完成后，在安全网关 IP 列表中，路由方式下的网口的 IP 将列在该物理网口设备下。</p> <p>设置为混合方式的网口，该界面显示的“网络接口”为“br:”+ 原物理网口设备名。安全网关 IP 配置完成后，在安全网关 IP 列表中，混合方式下的网口的 IP 将统一列在虚网口设备“br”下。</p>
接口 IP	<p>接口 IP 均设置在各个物理网口设备上。</p> <p>各个物理网口均可以配置多个 IP 地址。</p> <p>设置为混合模式的物理网口属于虚网口设备 br，原配置的 IP 地址将由 br 这个虚设备使用。br 也可以无 IP 地址。</p> <p> 不同物理网口设备上不能设置相同网段的 IP 地址。</p>

掩码	安全网关 IP 地址掩码																				
允许所有主机 PING	此项设置为允许后, 则任何主机都可以 ping 安全网关该网口上的该 IP 地址。																				
用于管理	指定用于管理后, 管理主机可以与该网口上的该 IP 地址进行通信。																				
允许管理主机 PING	此项设置为允许, 允许所有主机 PING 设置为不允许, 管理主机可以 ping 安全网关该网口上的该 IP 地址, 不是管理主机的则不能 ping 安全网关。																				
允许管理主机 Traceroute	<p>traceroute 含义: 管理员设置某个安全网关 IP 为可管理 IP 并允许 traceroute 后, 安全网关响应来自管理主机的目的地址为该 IP 的 traceroute 包, 其余情况如下表:</p> <table border="1" data-bbox="377 876 1163 1444"> <thead> <tr> <th rowspan="3">源 IP \ 目的 IP</th> <th colspan="3">安全网关 IP</th> <th rowspan="3">非安全网关 IP</th> </tr> <tr> <th colspan="2">可管理 IP</th> <th rowspan="2">非管理 IP</th> </tr> <tr> <th>允许管理主机 Traceroute</th> <th>禁止管理主机 Traceroute</th> </tr> </thead> <tbody> <tr> <td>管理主机</td> <td>允许</td> <td>禁止</td> <td>禁止</td> <td>走规则</td> </tr> <tr> <td>非管理主机</td> <td>禁止</td> <td>禁止</td> <td>禁止</td> <td>走规则</td> </tr> </tbody> </table>	源 IP \ 目的 IP	安全网关 IP			非安全网关 IP	可管理 IP		非管理 IP	允许管理主机 Traceroute	禁止管理主机 Traceroute	管理主机	允许	禁止	禁止	走规则	非管理主机	禁止	禁止	禁止	走规则
源 IP \ 目的 IP	安全网关 IP			非安全网关 IP																	
	可管理 IP		非管理 IP																		
	允许管理主机 Traceroute	禁止管理主机 Traceroute																			
管理主机	允许	禁止	禁止	走规则																	
非管理主机	禁止	禁止	禁止	走规则																	

	允许：安全网关响应 traceroute 包； 禁止：安全网关不响应 traceroute 包，也不转发 traceroute 包； 走规则：如果规则允许，安全网关不响应 traceroute 包，但允许转发到目的主机。
--	--

例如：

在“网络配置>>网络接口”界面中，分别将 FE1/FE2 设置为混合模式。

在“网络配置>>接口 IP”界面中点击添加，弹出“接口 IP 维护”界面，网络接口处会显示为“br: FE1”和“br: FE2”这样两个设备名。

接口 IP 配置完成后，在接口 IP 列表中会将已配置给“br: FE1”和“br: FE2”设备的 IP 地址显示在虚网口设备“br”下。

在“网络配置>>网络接口”中，将 FE1/FE2 由混合方式切换为路由方式后，配置在“br: FE1”上的 IP 将保留在 FE1 上，配置“br: FE2”上的 IP 将保留在 FE2 上。接口 IP 列表将自动更新显示。

注意：

接口 IP 在被安全规则引用以及被 HA 基本配置引用时，无法进行删除操作。

6.3. 网络配置>>策略路由

SecGate 3600-G10 安全网关提供策略路由机制，除常规的按目的 IP 方式的路由功能外和按源 IP 方式的路由功能。按源 IP 方式是根据数据帧中的源 IP 地址来决定下一跳地址。通过按源 IP 路由功能的有效补充，管理员可以方便的选择按源地址路由或

按目的地址路由，实现策略路由功能。

策略路由表包括：手工加入的静态路由表（分为源路由表项和路由表项）、系统根据安全网关 IP 地址自动加入的网段地址的路由表项。

当匹配多条路由时，按源路由、目的路由的顺序选择下一跳的地址。



策略路由的使用说明：

- 网口允许“按源路由”时，如果策略路由表中有匹配的源 IP 路由，则按源 IP 路由；无源 IP 路由匹配时，则按目的 IP 路由；无匹配目的 IP 路由时，则按默认网关路由。
- 网口禁止“按源路由”时，无论有无匹配的源 IP 路由时，均按匹配的目的 IP 路由；无匹配目的 IP 路由时，则丢弃该数据包。
- 网口配置中，默认路由的策略是源 IP 路由功能禁止，此时按目的 IP 地址路由。
- 策略路由功能和网口工作模式无关，也就是网口可以在路由模式，也可以在混合模式下，只要数据包需要进行路由，并且该网口开启了“按源 IP 路由”功能，那么就会匹配策略路由。

网络配置 >> 策略路由

以下网口是否允许按源IP路由



fe1 fe2 fe3 fe4 fe5 fe6 fe7 fe8 ge1 ge2 ge3


确定

类型	源地址	目的地址	下一跳	操作
路由	any	0.0.0.0/0.0.0.0	10.50.10.44	 

添加

域 名	说 明
-----	-----

以下网口是否允许按源IP路由	设置安全网关的所有网络接口是否启动按源 IP 路由
类型	静态路由分为：系统路由，目的路由，源路由
源地址	<p>当指定源 IP/掩码/下一跳网关，或者，源 IP/掩码/目的 IP/掩码/下一跳网关，表示按源 IP 路由。即，只要指定的内容有源 IP 地址，则按源 IP 地址路由。</p> <p>默认源 IP 地址为 any；最多能添加 1024 条源路由。</p>
目的地址	<p>当指定目的 IP/掩码/下一跳网关，表示按目的 IP 路由。即，只要指定内容中无源 IP 地址，则按目的 IP 地址路由。</p> <p>默认目的 IP 地址为 any。</p>
下一跳地址	<p>将指定的源 IP 地址的数据包，或者，将指定的目的 IP 地址的数据包，发送到该 IP 所在设备上。目的路由添加时，可以选择要走的 vpn 设备而不输入下一跳 IP 地址。</p>
操作	<p>可以添加、编辑、删除相关的静态路由表项</p> <p>系统路由表随着安全网关 IP 地址的配置自动更新，不需要管理员更新</p>

在“网络配置>>策略路由”，点击 ，在弹出的页面上方选择不同的路由方式，将会出现以下两种界面：



域 名	说 明
路由	按目的 IP 路由。
源路由	按源 IP 路由。
源地址	当指定源 IP/掩码/下一跳网关，或者，源 IP/掩码/目的 IP/掩码/下一跳网关，表示按源 IP 路由。即只要指定内容有源 IP 地址，则按源 IP 地址路由。 默认源 IP 地址为 any。
掩码	源地址的掩码。
目的地址	当指定目的 IP/掩码/下一跳网关，表示按目的 IP 路由。即只要指

	定内容中无源 IP 地址，则按目的 IP 地址路由。 默认目的 IP 地址为 any。
掩码	目的地址的掩码。
下一跳地址	将指定的源 IP 地址的数据包，或者，将指定的目的 IP 地址的数据包，发送到该 IP 所在设备上。当选中“路由”或“源路由”时，界面上只显示一个“下一条地址”。

6.4. 网络配置>>静态 ARP

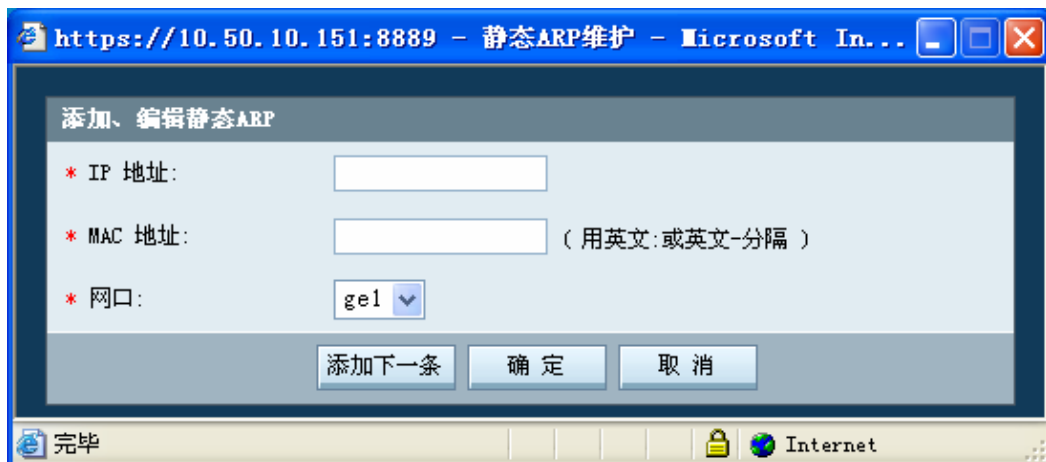
安全网关可以手工添加静态 ARP 表。当不希望 ARP 表超时，或者安全网关学习不到 ARP 时，可以采用添加静态 ARP 表的方式。ARP 表的显示界面如下：

网络配置>>静态ARP					请输入关键字	查找
序号	IP	MAC	网口	操作		
1	44.4.4.4	00:0C:29:F8:C8:E2	ge1			
2	5.5.5.5	00:0C:29:F8:C8:E2	ge1			
3	6.6.6.6	00:0C:29:F8:C8:E2	ge1			
4	6.6.6.7	00:0C:29:F8:C8:E2	ge1			
5	6.7.6.6	00:0C:29:F8:C8:E2	ge1			
6	7.7.7.7	00:0C:29:F8:C8:E2	ge1			
7	8.6.6.6	00:0C:29:F8:C8:E2	ge1			
8	8.8.8.8	00:0C:29:F8:C8:E2	ge1			
9	8.8.8.9	00:0C:29:F8:C8:E2	ge1			
10	9.9.9.8	00:0C:29:F8:C8:E2	ge1			
11	9.9.9.9	00:0C:29:F8:C8:E2	ge1			




 第1页/1页 跳转到 页 每页 行 

点击 **添加** 按钮，弹出下面的界面：



菜单说明：

域 名	说 明
IP 地址	ARP 表的 IP 地址
MAC 地址	与上述 IP 地址对应的 MAC 地址
网口	上述 IP 地址所对应的网口

6.5. 网络配置>>DHCP 配置

SecGate 3600-G10 安全网关全面支持 DHCP 功能，安全网关可以做为 DHCP 服务器，为外面的客户端动态分配 IP 地址。同时，安全网关还可以做为 DHCP 中继，为客户端和服务端转发 DHCP 请求和响应。

6.5.1.DHCP 配置>>DHCP 服务器

下面的界面是 DHCP 服务器的主界面

网络配置>>DHCP配置>>DHCP服务器							
DHCP域配置							
网络地址	网络掩码	网关地址	域名	DNS服务器	地址范围	备注	操作
无记录							
<input type="button" value="添加"/>							
静态IP地址							
主机名	MAC地址	IP地址		备注	操作		
无记录							
<input type="button" value="添加"/>							
启动/停止							
<input type="button" value="立即启动服务器"/>							
DHCP服务器已停止							

1. DHCP 域

点击 DHCP 域配置的添加按钮，弹出如下界面：

添加DHCP服务器域

VPN客户端:

VPN客户端子网掩码:

*网络地址:

*网络掩码:

网关地址:

域名:

DNS服务器:

*地址范围: ▼

备注:

菜单说明:

域 名	说 明
VPN 客户端	启用支持 VPN 客户端功能，提供 DHCP Over IPsec 功能
VPN 客户端子网掩码	若启用了上面的 VPN 客户端，则此输入框变为可输入，输入分配给 VPN 客户端的子网掩码。
网络地址	dhcp 要分配的网络地址，必须和接受 dhcp 请求的网口在同一网段。
网络掩码	与上面的网络地址相“与”，得到一个网段的地址

网关地址	为 dhcp 客户端配置网关，一般是安全网关接受 dhcp 请求的网卡地址，也可以是其他地址。
域名	为 dhcp 客户端配置域名（注意域名中不能有 ‘.’，否则启动失败）
DNS 服务器	为 dhcp 客户端配置 DNS 服务器
地址范围	地址范围，需要先在地址资源中定义的，直接选择。定义的范围必须和上面的网络地址在同一网段。
备注	说明信息

2. 静态 IP 地址

是指 dhcp 服务器为某个特定的 dhcp 客户端提供静态固定的 IP 地址。

点添加按钮，弹出如下界面：

编辑DHCP静态地址分配

*主机名称: (1-15位 字母、数字、减号、下划线的组合)

*MAC地址: (用英文:或英文-分隔)

*IP地址:

备注:

菜单说明：

域 名	说 明
-----	-----

主机名称	设置获取静态 IP 地址的主机名称
MAC 地址	为 dhcp 客户端设置固定的 MAC 地址
IP 地址	为 dhcp 提供静态的 IP 地址。
备注	说明信息

3. 启动 DHCP 服务器

立即启动服务器

当配置完所有信息，可以点击命令按钮立即启动服务器，即可启动安全网关上的 dhcp 服务器。



注意 DHCP 服务器启动前提条件：需要安全网关一个物理网口配置和 DHCP 地址范围一致，否则 DHCP 服务器无法启动

6.5.2.DHCP 配置>>DHCP 中继

网络配置>>DHCP配置>>DHCP中继

启动DHCP中继:

*DHCP服务器IP地址:

监听的接口: ▼

菜单说明：

域 名	说 明
-----	-----

启动 DHCP 中继	选上此复选框，点下面的确定，则启动 dhcp 中继功能。
DHCP 服务器 IP 地址	设置 dhcp 中继要代理的 dhcp 服务器 IP 地址
监听端口	与 dhcp 客户端连接的安全网关网口

7. VPN 配置

本章主要介绍 SecGate 3600-G10 安全网关 VPN（虚拟专用网络）功能的配置。VPN 功能使得用户可以在开放的 Internet 上基于 IPSec 的一系列加密认证以及密钥交换技术，构建一个安全的私有专网，具有同本地私有网络一样的安全性、可靠性和可管理性等特点，这样可以大大降低了企业/政府/科研机构等建设专门私有网络的费用。

SecGate 3600-G10 安全网关的 VPN 系统能提供基于 IPSec 协议的 VPN 功能。IPSec VPN 支持“网关到网关”和“客户端到网关”两种形式的隧道。为了建立这两种隧道，提供如下界面管理：VPN 的基本配置，VPN 客户端分组，VPN 端点的配置，VPN 隧道配置，VPN 策略和证书管理。

每次创建一条新的网关隧道或客户端隧道，通常按照下面步骤进行：

第一步：在“VPN 配置>>基本配置”页面，配置一些对 IPSec VPN 的基本设置，例如缺省 IPSec 协议要求的 IKE（Internet 密钥交换）密钥周期，是否启用 DHCP over IPSec 功能等。

第二步：在“VPN 配置>>VPN 端点”页面，添加远程 VPN 端点的基本信息，包括名称，地址方式，认证方式，密钥数据，IKE 算法模式和 IKE 算法组件等。

第三步：在“VPN 配置>>VPN 隧道”页面，添加 VPN 隧道，引用相应的 VPN 端点，设置数据包封装协议，IPSec 算法组件等信息。

第四步：配置相应的 VPN 策略，设置本地保护的网路地址和远端网路地址，引

用相应的 VPN 隧道。

如果在设置 VPN 端点时，“认证方式”设置为“证书”方式，就必须首先通过“证书管理”目录下的配置界面导入相应的 CA（认证中心）证书、本地证书、对方证书后，才可以建立使用证书方式进行认证。

对于“客户端到网关”隧道方式，可以通过“VPN 配置>>VPN 客户端分组”，对客户端进行分组，每组用户具有相同的 VPN 端点属性，同时又可以具有各自独立的证书或预共享密钥，这样可以大大方便了 VPN 客户端账号的管理。



如果使用“网关到网关”隧道方式，需要建立多条隧道时，对于每个远端的网关，只需要设置一个远程 VPN 端点，然后通过添加多个自动 IKE 隧道来引用该端点来实现。

下面详细介绍 VPN 配置中的每个 Web 界面的具体配置。

7.1. 基本配置

该页面主要配置 IPSec VPN 的基本功能和缺省参数。

VPN配置>>基本配置

是否启用VPN功能

启用VPN功能:

IPSec基本配置

本地VPN网关IP地址:

VPN状态:

VPN卡所在网口:

默认预共享密钥: (6-128个字符, 更新后, 请在远端隧道端点中重新编辑相应的记录)

默认IKE密钥生存期: (1200-86400秒)

默认IPSec密钥生存期: (1200-86400秒)

DHCP over IPSec配置

启用DHCP over IPSec功能:

DHCP服务器的IP地址:

DHCP中继设备接口:

说明: 如果选择本设备的DHCP服务器, 请填写服务器地址为127.0.0.1, 中继设备接口为本地回环设备1o.

VPN 基本配置菜单说明:

域 名	说 明
启用 VPN 功能	是否启用 VPN 功能
本地 VPN 网关 IP 地址	VPN 接口的 IP 地址, 应该和“网络配置>>安全网关 IP”中该接口的 IP 地址一致
VPN 状态	VPN 的工作状态, 为“启用”或“未启用”
VPN 卡所在网口	VPN 卡出厂时在安全网关上所位于的网口, 默认为 GE1, 不可修改。
默认预共享密钥	预共享密钥, 在此处修改了预共享密钥后, 原先使用了修改前的预共享密钥的 VPN 端点继续使用原预共享密钥, 如果需要, 请到“VPN 配置>>VPN 端点”中重新编辑用到预共享密钥的条目, 其它类似。

域 名	说 明
默认 IKE 密钥生存期	IKE 密钥生命周期，单位为秒，必须在 [1200, 86400] 之间
默认 IPSec 密钥生存期	IPSec 密钥生命周期，单位为秒，必须在 [1200,86400] 之间
启用 DHCP over IPSec 功能	选择启用后可以为 VPN 客户端动态分配内部 IP 地址。
DHCP 服务器的 IP 地址	为 VPN 客户端动态分配内部 IP 地址的 DHCP 服务器地址。
DHCP 中继设备接口	从安全网关到达 DHCP 服务器的网口，如果使用安全网关自身的 DHCP 服务器，中继设备选择本地接口“lo”。

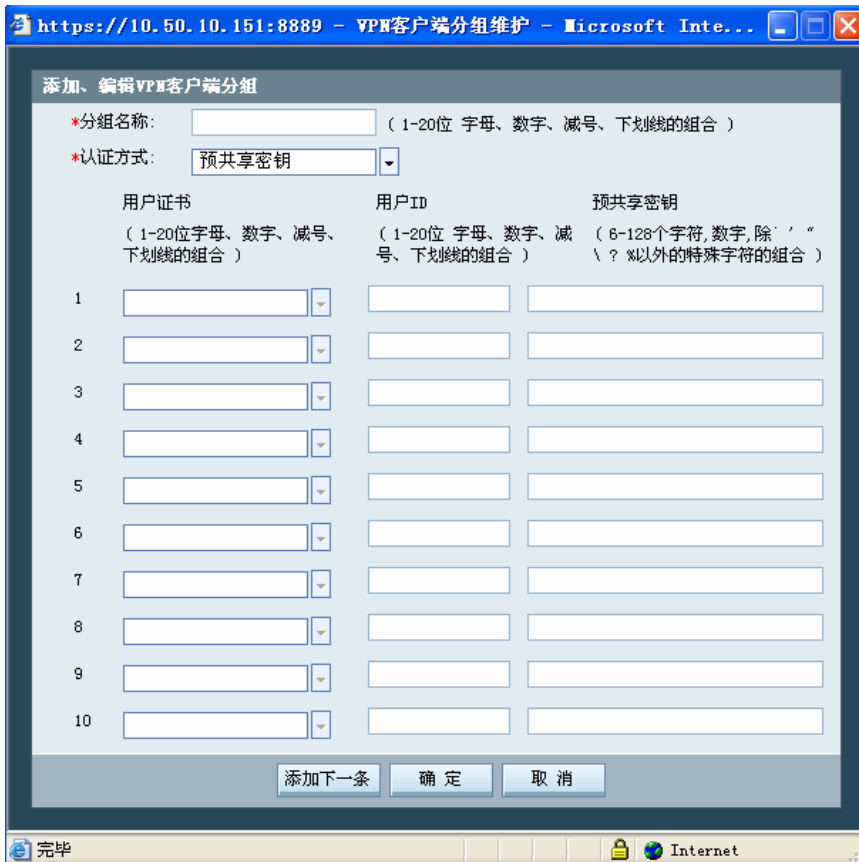
7.2. VPN 客户端分组

在使用 VPN 客户端访问企业内部网络时，主要针对很多出差、家庭办公、远程办公的用户，或者小型分支机构。网络管理员需要为这些用户设置建立 VPN 的共享密钥或者证书。如果为每一个远程客户端用户单独设置 VPN 端点配置、VPN 隧道、VPN 策略，这样就增加了管理员的工作量。使用 VPN 客户端分组配置可以首先对众多具备一致 VPN 端点属性的用户分组，减少在后续中的配置工作量。

该页面如下所示：




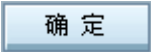
点击 **添加** 按钮，弹出“VPN 客户端分组维护”窗口，填写分组名称，认证方式和每个用户的证书或预共享密钥：



菜单说明：


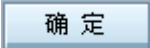
域 名	说 明
分组名称	VPN 客户端名称，唯一标识，符合命名规则（1—20 个字母、数字、减号、下划线组合）
认证方式	预共享密钥或证书
用户证书	分组中该用户使用的证书名称
用户 ID	分组中该用户的用户名
预共享密钥	分组中该用户名对应的预共享密钥

编辑 VPN 客户端分组

1. 点击想要对其进行编辑的 VPN 客户端分组的“编辑”图标 ，弹出“VPN 客户端分组维护”窗口。
2. 修改完成后，点击  按钮。

菜单说明，同“添加 VPN 端点”。

删除 VPN 客户端分组

1. 点击想要进行删除的 VPN 客户端分组的“删除”图标 ，在弹出的对话框中点击 。

2. 删除成功，则关闭对话框。







7.3. VPN 端点

在建立 VPN 隧道之前，必须明确每条隧道都要有两个端点。其中一个端点是正在配置的该安全网关设备，另外一个远程端点这里称为“VPN 端点”。隧道两端都必须进行相同属性的配置，才可以正常地建立起隧道。用户首先要输入其要建立隧道的 VPN 端点信息。对端是隧道的终点，由它来负责传去的加密报文的解密和传回报文的加密。远程 VPN 端点有两种类型，一种是网关，一种是客户端；前者通常就是一台类似 SecGate 3600-G10 安全网关的专门 VPN 网关设备，后者通常是指客户主机，通常是一台台式计算机或笔记本电脑。

VPN配置>>VPN端点		请输入关键字		查找		
VPN端点名称	类型	地址形式	IP地址或组	认证方式	状态	操作
广州	网关	静态IP地址	101.101.101.101	预共享密钥		 
上海	网关	静态IP地址	202.202.202.202	预共享密钥		 

第1页/1页 跳转到 1 页 确定 每页 全部 行

图标说明：

图 标	说 明
	启用状态，表示已生效
	启用状态，表示未生效
	编辑本条记录
	删除本条记录

VPN 菜单说明：

域 名	说 明
VPN 端点名称	VPN 端点名称，唯一标识，符合命名规则（1—20 个字母、数字、减号、下划线组合）
类型	网关或者客户端
地址形式	动态 IP 地址或静态 IP 地址
IP 地址或组	VPN 端点的 IP 地址或所属分组
认证方式	与 VPN 端点进行相互认证的方式，预共享密钥或者是证书

域 名	说 明
状态	该 VPN 端点是否已经生效
操作	编辑或删除

添加 VPN 端点

添加 VPN 端点时，需要根据实际情况选择合适的类型和认证方式。当用户选择的是客户端类型，或 VPN 端点地址为“0.0.0.0”，且“认证模式”为“主模式”时，只能使用证书认证方式。当用户选择“认证方式”为“证书”时，需要指定相应的本地证书和对方证书。SecGate 3600—G10 安全网关支持 7 类远程 VPN 端点类型组合，如下表示：

编号	类型	隧道认证方式	认证类型
1	静态类型 (static)	主模式 (main)	预共享密钥 (psk)
2			证书 (rsasig)
3		野蛮模式 (aggr)	预共享密钥 (psk)
4			证书 (rsasig)
5	动态类型 (dynamic)	主模式 (main)	证书 (rsasig)
6		野蛮模式 (aggr)	预共享密钥 (psk)
7			证书 (rsasig)

1. 点击“添加”按钮，弹出“VPN 端点维护”的窗口。
2. 输入完成后，点击“确定”按钮，或点击“添加下一条”按钮，添加下一个 VPN 端点。




菜单说明：

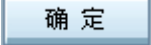
域 名	说 明
-----	-----

域 名	说 明
VPN 端点名称	VPN 端点名称，唯一标识，符合命名规则，必须是 1—20 位字母、数字、减号、下划线、中文字符的组合，不能为空。
类型	网关或客户端
地址形式	选择 VPN 端点的地址表示形式，可选内容为“静态 IP 地址”或“动态 IP 地址”。
IP 地址	当远程 VPN 地址形式为“静态 IP 地址”，此处输入远程 VPN 的 IP 地址或者域名。
用户组	当 VPN 端点类型是“客户端”时，这里可以选用已定义的 VPN 客户端分组。
认证方式	与 VPN 端点进行相互认证的方式，可选内容为“预共享密钥”或“证书”
预共享密钥	当认证方式为“预共享密钥”，此处输入预共享密钥的值。缺省为“VPN 配置>>基本配置>>IPSec”中设置的预共享密钥的值。
本地证书	当认证方式为“证书”时，在此处选择本地证书，可选内容为：在“VPN 配置>>证书管理>>本地证书”中生成的证书。
远端证书	当认证方式为“证书”时，在此处选择对方证书，可选内容为：在“VPN 配置>>证书管理>>对方证书”中生成的证书。
IKE 算法模式	IKE 协商第一阶段的认证模式，可选内容为“主模式”和“野蛮模式”。主模式需要三个交换完成 IKE SA（安全联盟）的建立，提供交换

域 名	说 明
	双方的身份保护。野蛮模式只需要一个交换就可以完成 IKE SA 的建立，不提供身份保护
本地 ID	本地网关的设备 ID，必须是 1—20 位字母、数字、减号、下划线的组合，不能为空
对方 ID	远程 VPN 网关的设备 ID 或远程 VPN 用户的用户 ID，必须是 1—20 位字母、数字、减号、下划线的组合，不能为空
启用 NAT 穿越	与 VPN 端点建立隧道是否需要 NAT 穿越
IKE 算法组件	IKE 协商第一阶段加密和认证算法选择。最多可以选择 8 种提案。
IKE 密钥生存期	第一阶段协商密钥生存周期，在此周期结束后将重新进行 VPN 双方的认证。
远端状态探测 (DPD)周期	VPN 建立之后，为了在异常网络环境下正确使用。达到双方同步，需要周期性的探测远程 VPN 是否在线。
远端状态探测 (DPD)超时	如果在这段时期内没有探测到远程的在线情况，则将这条隧道超时删除。

编辑 VPN 端点

1. 点击想要对其进行编辑的 VPN 端点的“编辑”图标 ，弹出“VPN 端点维护”的窗口。


2. 修改完成后，点击  按钮。

菜单说明，同“添加 VPN 端点”。



在编辑 VPN 端点后，需要重新生效相应的 VPN 隧道后，修改的 VPN 端点信息才会生效。

删除 VPN 端点

1. 点击想要进行删除的远程 VPN 的“删除”图标 ，在弹出的对话框中点击



2. 删除成功，则关闭对话框。



当删除 VPN 端点时，将删除所有的和此 VPN 端点相关的 VPN 隧道。





7.4. VPN 隧道

VPN 隧道是指在 SecGate 3600—G10 安全网关和 VPN 端点之间通过周期性的自动密钥交换（IKE）建立的高安全性的加密通道。隧道根据 VPN 端点的类型可以分为两类，一种是网关到网关之间建立的隧道，用于保护两个子网之间的数据通信，另一种是客户端和网关之间建立的隧道，用于保护内部子网和远程主机之间的数据通信。

VPN配置 >> VPN隧道					
隧道名称	本地网关地址	远端隧道端点	封装协议	状态	操作
to-guangzhou	10.50.10.237	广州	esp		 
to-shanghai	10.50.10.237	上海	esp		 

第1页/1页 跳转到 1 页 确定 每页 全部 行

图标说明：

图 标	说 明
	启用状态，表示已生效
	启用状态，表示未生效
	编辑本条记录
	删除本条记录

VPN 隧道菜单说明：

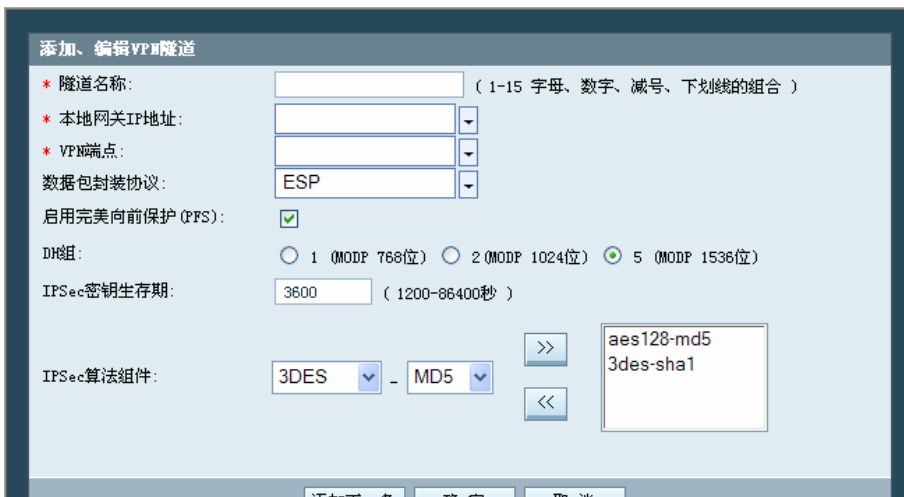
域 名	说 明
隧道名称	网关隧道名称，唯一标识，符合命名规则

本地网关地址	自动读取“VPN 配置>>基本配置”中的本地 VPN 网关 IP 地址
远端隧道端点	要建立隧道的对方 VPN 端点
封装协议	ESP 或 AH
状态	该 VPN 隧道是否已经生效
操作	编辑或删除

添加 VPN 隧道

在添加 VPN 隧道时，设置对数据隧道进行加密、认证、密钥生存期等属性。

1. 点击“添加”按钮，弹出“VPN 隧道维护”窗口。
2. 输入完成后，点击“确定”按钮，或“添加下一条”按钮，添加下一个 VPN 隧道。



The screenshot shows the '添加、编辑VPN隧道' (Add/Edit VPN Tunnel) configuration window. It contains the following fields and options:

- 隧道名称:** Text input field with a note: (1-15 字母、数字、减号、下划线的组合)
- 本地网关IP地址:** Dropdown menu
- VPN端点:** Dropdown menu
- 数据包封装协议:** Dropdown menu (ESP selected)
- 启用完美向前保护(PFS):** Checked checkbox
- DH组:** Radio buttons for 1 (MODP 768位), 2 (MODP 1024位), and 5 (MODP 1536位) (5 is selected)
- IPSec密钥生存期:** Text input field (3600) with a note: (1200-86400秒)
- IPSec算法组件:** Two dropdown menus (3DES and MD5) with '>>' and '<<' buttons. A preview box shows 'aes128-md5' and '3des-sha1'.


菜单说明:

域 名	说 明
隧道名称	网关隧道名称，唯一标识，符合命名规则，必须是 1—20 位字母、数字、减号、下划线的组合，不能为空。
本地网关 IP 地址	自动读取“VPN 配置>>基本配置”中的本地 VPN 网关 IP 地址
远端隧道端点	要建立隧道的对方 VPN 端点名称
数据包封装协议	可选内容为：“ESP”，“AH”。AH 协议提供无连接的完整性、数据源认证和抗重放保护服务，ESP 提供和 AH 类似的服务，并增加了数据保密和有限的数据流保密服务
IPSec 算法组件	数据通信和认证时的加密算法。可选内容为：3des-md5，3des-sha1，aes128-md5，aes128-sha1，aes256-md5，aes256-sha1，null-md5，null-sha1。
启用完美前向保护 (PFS)	是否选用完美前向保密方式，隧道两端该参数的选择应该一致，否则无法建立隧道。
DH 组	在进行第二阶段密钥协商时使用的 DH 交换组
IPSec 密钥生存期	IPSec 密钥生存周期




网络中间如果有 NAT 设备，则数据包认证方式无法使用 AH 协议，国际标准不支持 AH 数据包穿越 NAT。

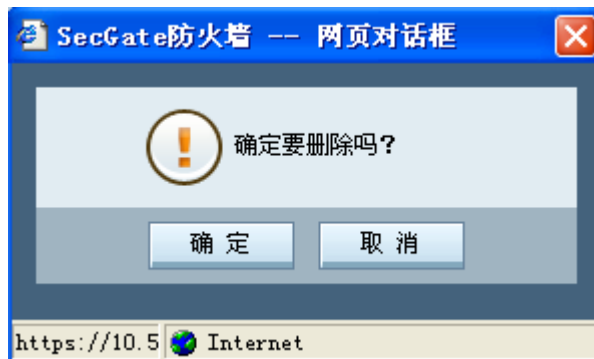
编辑 VPN 隧道

1. 点击想要对其进行编辑的 VPN 隧道的“编辑”图标 ，弹出“VPN 隧道维护”窗口。
2. 修改完成后，点击“确定”按钮。

菜单说明，同“添加 VPN 隧道”。

删除 VPN 隧道

1. 点击想要进行删除的网关隧道“删除”图标 ，在弹出的对话框中点击“确认”。
2. 删除成功，则关闭对话框。



7.5. VPN 策略

VPN配置>>VPN策略					
策略名	源地址	目的地址	隧道名	状态	操作
3ewe	4.4.44.4	6.6.6.6	3wfd		 
<input type="button" value="添加"/>					
第1页/1页 跳转到 <input type="text" value="1"/> 页 确定 每页 <input type="text" value="全部"/> 行					

图标说明:

图 标	说 明
	启用状态，表示已生效
	启用状态，表示未生效
	编辑本条记录
	删除本条记录

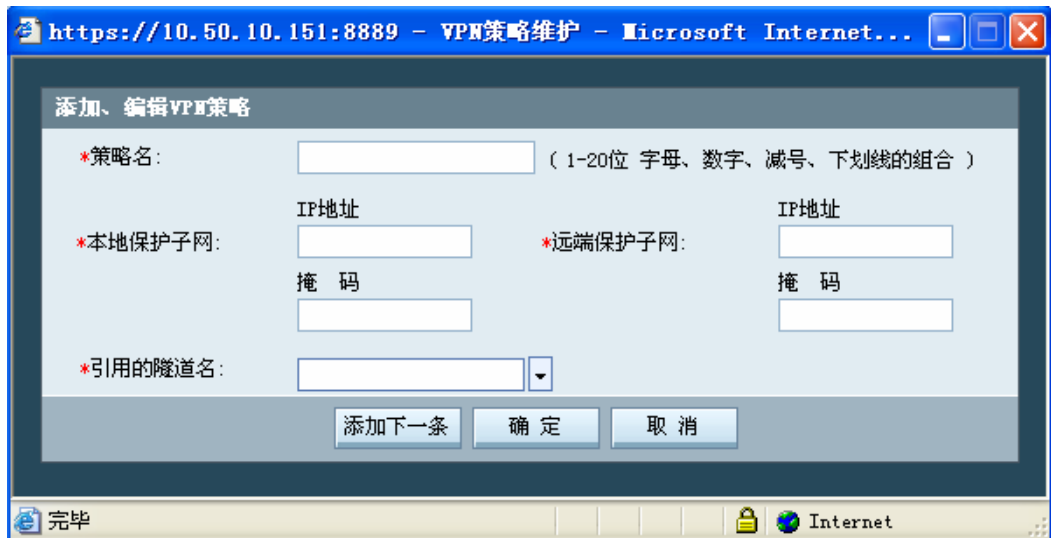
菜单说明:

域 名	说 明
策略名	VPN 策略名称，唯一标识，符合命名规则
源地址	本地需要保护的子网网段
目的地址	远程 VPN 端点的内部网段
隧道名	使用的隧道名
状态	这条策略是否已经被生效

域 名	说 明
操作	编辑、删除

添加 VPN 策略

1. 点击“添加”按钮，弹出“VPN 策略维护”窗口。
2. 输入完成后，点击“确定”按钮，或点击“添加下一条”按钮，添加下一个 VPN 策略。




菜单说明：

域 名	说 明
策略名	VPN 策略名称，唯一标识，符合命名规则，必须是 1—20 位字母、数字、减号、下划线的组合，不能为空。
本地保护子网	本地安全网关后的子网网段。
远程保护子网	远程 VPN 的内部网段


域 名	说 明
引用的隧道	此策略中数据要通过的隧道。

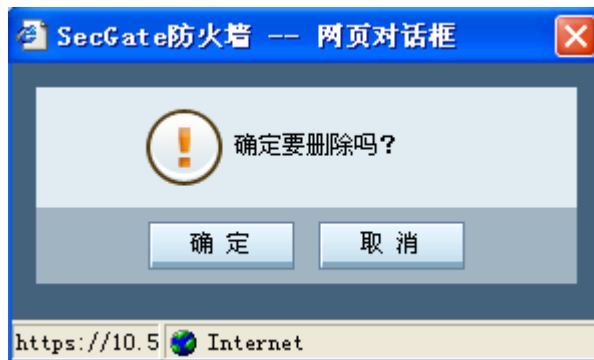
编辑 VPN 策略

1. 点击想要对其进行编辑的 VPN 策略的“编辑”图标 ，弹出“VPN 策略维护”窗口。
2. 修改完成后，点击“确定”按钮。

菜单说明，同“添加 VPN 策略”。

删除 VPN 策略

1. 点击想要进行删除的客户端隧道的“删除”图标 ，在弹出的对话框中点击“确认”。
2. 删除成功，则关闭对话框。



7.6. 证书管理

证书管理包括：CA 证书，本地证书，对方证书和证书吊销列表。CA 证书是进行认证的基础，利用他验证对方证书是否可信。本地证书是 VPN 的证书，VPN 利用本地证书与远程 VPN 交换身份信息，进行认证。VPN 使用对方证书或对方证书主题判断对方证书身份是否合适。证书吊销列表是证书管理中心已经吊销的证书列表，防止对端使用已经吊销的证书。

用户应该首先添加合适的 CA 证书，其次再添加该 CA 证书签发的本地证书和对方证书。可以通过“VPN 配置>>证书管理>>CA 证书”，“VPN 配置>>证书管理>>对方证书”和“VPN 配置>>证书管理>>本地证书”与 CA 软件相配合，来生成和导出证书。如果有吊销的证书，还必须导入证书吊销列表。

7.6.1. 证书管理>>CA 证书

VPN配置>>证书管理>>CA证书				
名称	颁发者	主题	有效期起始时间	有效期终止时间
<input type="checkbox"/>	C=CN, cacert CN=CARoot/Email=CARoot@legend.com	C=CN, CN=CARoot/Email=CARoot@legend.com	May 14 01:23:22 2002 GMT	Jun 10 01:23:22 2012 GMT
<input type="checkbox"/> 全选 <input type="button" value="导入"/> <input type="button" value="删除"/> <input type="button" value="导出证书"/>				
第1页/1页 跳转到 1 页 确定 每页 全部 行				

菜单说明：

域 名	说 明
名称	证书的名称，唯一标识，符合命名规则

域 名	说 明
颁发者	签发该证书的实体的惟一名 (DN)
主题	被授予该证书的实体的惟一名 (DN)
有效期起始时间	证书有效期开始的日期
有效期终止时间	证书有效期结束的日期

功能说明：

图 标	说 明
<input type="checkbox"/> 全选	选定所有的 CA 证书，或取消所有的 CA 证书的选定
导入	导入 CA 证书。可以使用证书管理器导出 CA 根证书，然后在此导入。如果使用第三方 CA，则导入第三方 CA 证书。
删除	删除选定的 CA 证书
导出证书	导出选定的 CA 证书

7.6.2. 证书管理>>对方证书

添加对方证书有两种方法，添加主题方式和导入方式。添加主题就是根据对方证书设置各种信息。VPN 认证对方身份时，判断对方证书是否和您在此添加的主题信息相符合。导入方式是把对方证书导入到 VPN，取出证书的主题，用主题来判断对方身份。




菜单说明：

域 名	说 明
名称	证书的名称，唯一标识，符合命名规则
颁发者	签发该证书的实体的唯一名（DN）
主题	被授予该证书的实体的唯一名（DN）
有效期起始时间	证书有效期开始的日期
有效期终止时间	证书有效期结束的日期

功能说明：

图 标	说 明
<input type="checkbox"/> 全选	选定所有的对方证书，或取消所有的对方证书的选定
添加主题	添加主题。VPN 认证对方身份时，判断对方证书是否和您在此添加的主题相符合。
导入	导入对方证书。将对方证书导入到 VPN，取出证书的主题，用此主题判断对方身份。
删除	删除选定的对方证书

图 标	说 明
	导出选定的对方证书

添加主题



https://10.50.10.151:8889 - 添加主题 - Microsoft Inter...

添加主题

* 证书名称: (1-20 字母、数字、减号、下划线组合)

国家:

省:

市区:

组织:

部门:

*公共名主题:

邮件:

完毕 Internet

菜单说明:

域 名	说 明
证书名称	证书的名称, 唯一标识, 符合命名规则
国家	证书被授予者所在的国家代码
省	证书被授予者所在的省的代码

域 名	说 明
市区	证书被授予者所在的市或区的代码
组织	证书被授予者所在的组织的代码
部门	证书被授予者所在的部门代码
公共名主题	证书被授予者的通用名或常用名
邮件	证书被授予者的电子邮箱地址

7.6.3. 证书管理>>本地证书

有两种添加本地证书的方法：密钥本地生成、密钥外部生成。一般情况下使用密钥本地生成。

使用密钥本地生成，VPN 内部随机生成公、私钥对，然后用公钥和您输入的请求信息生成证书请求文件。您将此证书请求文件导出后，可以在另外的证书管理器软件中签发，也可以用第三方 CA 签发。签发后将生成证书文件，将此证书文件导入到 VPN 就完成了本地证书生成的过程。

使用密钥外部生成，您可以将其他 CA 生成的证书、私钥导入到 VPN。



菜单说明：

域 名	说 明
名称	证书的名称，唯一标识，符合命名规则
颁发者	签发该证书的实体的唯一名（DN）
主题	被授予该证书的实体的唯一名（DN）
有效期起始时间	证书有效期开始的日期
有效期终止时间	证书有效期结束的日期

图标说明：

图 标	说 明
<input type="checkbox"/> 全选	选定所有的 CA 证书，或取消所有的 CA 证书的选定
密钥本地生成	如果密钥是在本地生成的，点击此按钮生成请求文件
密钥外部生成	如果密钥是在外部生成的，点击此按钮导入证书及密钥
导入	选定相应的请求文件前的复选框，点击此按钮导入本地证书
删除	删除选定的本地证书
导出证书	导出选定的本地证书，如果选定的是请求文件，则该按钮不起作用
导出请求文件	导出选定的请求文件，如果选定的是密钥外部生成的证书，则该按钮不起作用

密钥本地生成



密钥本地生成

* 证书名称: (1-20 字母、数字、减号、下划线组合)

国家:

省:

市区:

组织:

二级组织:

*公共名主题:

邮件:

生成请求文件 取消

Internet

菜单说明:

域 名	说 明
证书名称	证书的名称，唯一标识，符合命名规则
国家	证书被授予者所在的国家代码
省	证书被授予者所在的省的代码
市区	证书被授予者所在的市或区的代码
组织	证书被授予者所在的组织的代码
二级组织	证书被授予者所在的二级组织的代码

域 名	说 明
公共名主题	证书被授予者的通用名或常用名
邮件	证书被授予者的电子邮箱地址

7.6.4. 证书管理>>证书吊销列表



名称	颁发者	上次更新时间	下次更新时间
<input type="checkbox"/> dxcert	/C=CN/CN=CARoot/Email=CARoot@legend.com	Feb 16 08:43:51 2006 GMT	Feb 16 08:43:51 2007 GMT

全选

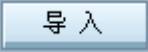

第1页/1页 跳转到 1 页 确定 每页 全部 行

菜单说明：

域 名	说 明
名称	证书的名称，唯一标识，符合命名规则
颁发者	签发该证书的实体的唯一名（DN）
上次更新时间	上次更新时间
下次更新时间	下次更新时间

功能说明：

图 标	说 明
<input type="checkbox"/> 全选	选定所有的吊销证书列表，或取消所有的吊销证书列表的选定

图 标	说 明
	点击此按钮导入吊销证书列表
	删除选定的吊销证书列表

8. 对象定义

为简化安全网关安全规则的维护工作，引入了对象定义，可以定义以下对象：

- (1) 地址：地址列表、地址组、服务器地址、NAT 地址池
- (2) 服务：服务列表、服务组
- (3) 代理：预定义代理、自定义代理
- (4) 时间：时间列表、时间组
- (5) 带宽：带宽列表
- (6) URL 列表：黑名单、白名单



- (1) 定义规则前需先定义该规则所要引用的对象。
- (2) 定义的对象只有被引用时才真正使用。
- (3) 被引用的对象编辑后，在“安全策略>>安全规则”界面中点击“刷新”后生效。

8.1. 对象定义通用功能介绍

对于各项对象，操作基本相同，通常提供如下操作：

- (1) 分页显示
- (2) 查找

- (3) 排序
- (4) 添加对象
- (5) 编辑对象（修改）
- (6) 删除对象

还有一些需要注意的地方，适用于所有的规则，比如：名称的限制、备注






下面对这些共同的功能做一个介绍。


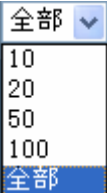


8.1.1.分页显示

各列表界面均有“分页功能”，其工具条通常位于表格的下方，如下图所示：




例如，点击“对象定义>>地址>>地址列表”，显示地址列表页面，就能看到上述工具条。实际上，所有对象的列表页面都有该项功能。具体说明如下：

操作功能	说 明
	首页
	上一页
	下一页
	尾页
	当前页面/总页码

	<p>当有很多页时，可以直接跳转。输入希望跳转的页码，点击 确定 即可。</p> <p>页码框只接受正整数。</p> <p>如果输入页面大于总页码，则跳转到最后一页。</p>
	<p>每页显示的行数</p>
	<p>如果出现竖向滚动条，则点击  可以回到该页页首。</p>

8.1.2. 查找

为便于查找已经定义过的对象，各列表界面均提供了查找功能，通常位于标题和列表之间，靠右排列。如下图所示：



具体说明如下：


操作功能	说明
查找	<p>通常为按“名称”和“备注”进行查找。</p> <p>在输入框中输入待查找的关键词，点击“查找”即可。</p> <p>如果输入框中为空或者默认值，则不进行筛选，列出所有对象。</p>

8.1.3. 排序


为便于查看比较对象，各列表界面均提供了排序功能。具体说明如下：

操作功能	说 明
排序	<p>在列表的标题部分，有两种不同格式的字体，如图所示</p> <p>序号 名称</p> <p>1 DMZ ，加下划线的（如名称）表示可以进行排序，没有加下划线的（如序号）则不能进行排序。用鼠标点击（如名称）则进行排序，升序降序交替进行，如前一次为升序排序，则下一次为降序排序。</p> <p>通常按照字符串顺序进行排序（如名称、备注，如果为数字项，则按数字大小进行排序（如端口）。</p>



8.1.4. 添加

各个对象最重要的操作之一就是能够添加对象，按钮都排列在各列表最下方的正中。

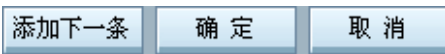
添加对象的操作步骤：

1. 在相应的对象列表页面中，点击，将弹出添加界面；

2. 给弹出界面的各域选择或者输入相应的值；

3. 点击 ，则成功添加本条规则后关闭本窗口；如果点击 ，则添加本条规则成功后刷新列表页码，本窗口不关闭，以便继续添加下一条。

点击  后弹出界面中最下方通常有三个按钮，如下图所示：





操作功能	说 明
添加下一条	<p>点击“添加下一条”，如果通过有效性检查，添加成功，则刷新列表界面，本窗口继续存在，可以继续添加新的对象。“添加下一条”通常用在同时添加若干对象的情况，无需再点击列表界面的“添加”按钮，简化了操作过程。</p> <p>在修改对象时，弹出窗口中只有“确定”和“取消”按钮，无“添加下一条”按钮。</p>
确定	<p>点击“确定”，如果通过有效性检查，添加成功，则关闭弹出窗口，刷新列表界面。“确定”为默认操作。</p>
取消	<p>点击“取消”，则关闭弹出窗口，即为取消本次操作。</p>

8.1.5.编辑（修改）

各个对象，不管是否被引用，均能随时修改。

编辑对象的操作步骤：




操作

1. 在相应的对象列表页面中，点击对应的编辑图标（如图： ），将弹出编辑界面；

2. 输入相应的值，或者指定相应的成员（对于各项对象，值的限制不同，在各对象中进行介绍，可参考具体对象的帮助或者手册）；

3. 点击 ，修改成功后关闭本窗口。



具体说明如下：

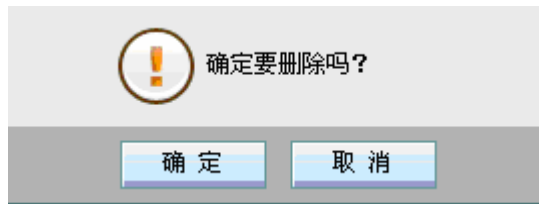
操作功能	说 明
编辑（修改）	<p>操作</p> <p>点击对应对象的   后，将弹出编辑框，通常，编辑框比添加框少一个  按钮，其它各项相同。</p> <p>需要注意以下三点：</p> <p>(1) 修改时，不能修改对象的名称，其它各项值均可修改。</p> <p>(2) 所有对象可以随时进行修改。例如，有一个地址“DepA”，不管它是否被安全规则等使用了，都可以进行修改。</p> <p>(3) 被引用的对象编辑后，在“安全策略>>安全规则”界面中点击“刷新”后生效。</p>

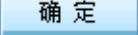
8.1.6.删除

对象可以被删除，但是被引用的对象不能被删除。删除对象的操作步骤如下：

操作

1. 在相应的对象列表界面，点击对应的删除图标（如图： ）；
2. 弹出确认框，如下图所示：



3. 点击  则进行删除动作，如果该对象不能被删除，则报告错误；如果点击“取消”，则取消本次操作。



被引用的对象不能被删除。有两种引用方式：

1. 被安全规则引用：即规则中使用了该对象；
2. 被组引用：即该对象为对象组的成员。

例如：

有一个地址“DepA”，如果其被安全规则等使用了，则不能进行删除。又如，地址“DepA”是地址组“GrpA”的成员，则不能删除地址“DepA”，要删除地址“DepA”，必须先地址组“GrpA”中移除该成员。

如果确实需要删除该对象，则必须清除对该对象的所有引用。

8.1.7. 名称和备注

值 域	说 明
名称	<p>所有对象都有名称，名称为必填项。</p> <p>名称不能被修改。如果确实需要修改名称，则只能先删除该对象，再重新添加。</p> <p>名称必须满足：1-20 字母、数字、减号、下划线组合。</p> <p>相同类型中不能重名，比如不能在地址列表中同时出项两个名称为“AAA”的地址，也不能在地址列表和地址组中出现同名。</p>
备注	<p>所有对象都有备注，备注为可选项。</p> <p>备注中不像名称那样对输入字符串进行了严格的限制，备注中可以输入任何字符，但是必须小于等于 255 个字节，即 255 个英文字符或者 127 个汉字。</p>

8.2. 地址

在定义安全规则之前，最好按照一定的原则（比如：按部门、按人员等）定义一些地址，这样，当部门或者人员的 IP 地址发生变化时，只需在本列表中更新即可，无需再修改安全规则了。

在“对象定义>>地址”中，定义了三种不同用途的地址：

1. 地址列表、地址组：用于“安全策略>>安全规则”中的源地址和目的地址，“用



户认证>>用户列表”和“用户认证>>用户组”中的安全策略。

2. 服务器地址：用于“安全策略>>安全规则”中的内部地址。
3. NAT 地址池：用于“安全策略>>安全规则”中的源地址转换。

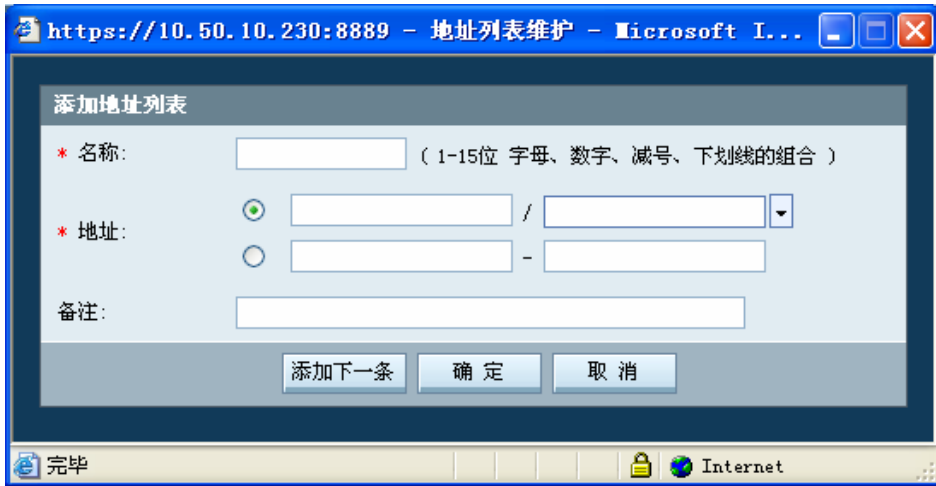
8.2.1.地址>>地址列表

地址用于“安全策略>>安全规则”、“用户认证>>用户列表”和“用户认证>>用户组”。

可以按两种方式来定义地址：（1）IP 地址/掩码；（2）地址范围 IP1-IP2

序号	名称	地址	备注	操作
1	DMZ	192.168.11.1 - 192.168.11.3	DMZ区	 
2	trust	192.168.10.1 - 192.168.10.100	内网	 
3	untrust	10.50.11.0 / 255.255.255.0	untrust区	 

在“对象定义>>地址>>地址列表”界面中，点击 ，将弹出以下界面：







值 域	说 明
名称	地址的名称，必须满足：1-20 位字母、数字、减号、下划线组合。
地址	<p>IP 地址。</p> <p>两种添加 IP 地址的方式：</p> <p>（1）IP/MASK 方式：自动应用 IP 和掩码运算来表示一个网段。例如：输入 192.168.25.22/255.255.255.0，则添加成功后变为 192.158.25.0/255.255.255.0。</p> <p>如果希望指定一台主机，请选择掩码为 255.255.255.255。</p> <p>（2）IP1-IP2 方式：IP1 必须小于或等于 IP2。如果只指定一台主机，可以让 IP1 和 IP2 相等。</p>
备注	备注为可选项。备注中可以输入任何字符，但是必须小于等

于 255 个字节，即 255 个英文字符或者 127 个汉字。

8.2.2.地址>>地址组

地址组用于“安全策略>>安全规则”、“用户认证>>用户列表”和“用户认证>>用户组”。

地址组的成员只能为“对象定义>>地址>>地址列表”中已经定义过的地址。

序号	名称	成员	备注	操作
1	dmzgrp	DMZ	服务器组	 
2	trustgrp	trust	内部网	 





在“对象定义>>地址>>地址组”界面中，点击 ，将弹出以下界面：



值 域	说 明
-----	-----

地址列表	列出所有在“对象定义>>地址>>地址列表”中定义的地址，“服务器地址”和“NAT 地址池”不能作为地址组的成员。 被添加到地址组成员列表中的地址将不再显示在地址列表中。
地址组成员	属于该地址组的所有成员。 成员只能是在“对象定义>>地址>>地址列表”中定义的地址。 地址组至少要有一个成员。

提供以下操作：

操作功能	说 明
	添加成员，点击  把选中的地址添加到成员列表
	删除成员，点击  把选中的成员移回到地址列表中

8.2.3.地址>>服务器地址

在“安全策略>>安全规则”中的

安全规则维护

*规则序号:

规则名: (1-15位 字母、数字、减号、下划线的组合)

类型:

条件

源地址:

*公开地址:

操作

源地址转换为:

*公开地址映射为:

VPN隧道: 日志记录:

>>高级选项

安全规则维护

*规则序号:

规则名: (1-15位 字母、数字、减号、划划线的组合)

类型:

条件

源地址:

* 对外服务:

* 公开地址:

操作

源地址转换为:

*公开地址映射为:

*对外服务映射为:

VPN隧道: 日志记录:

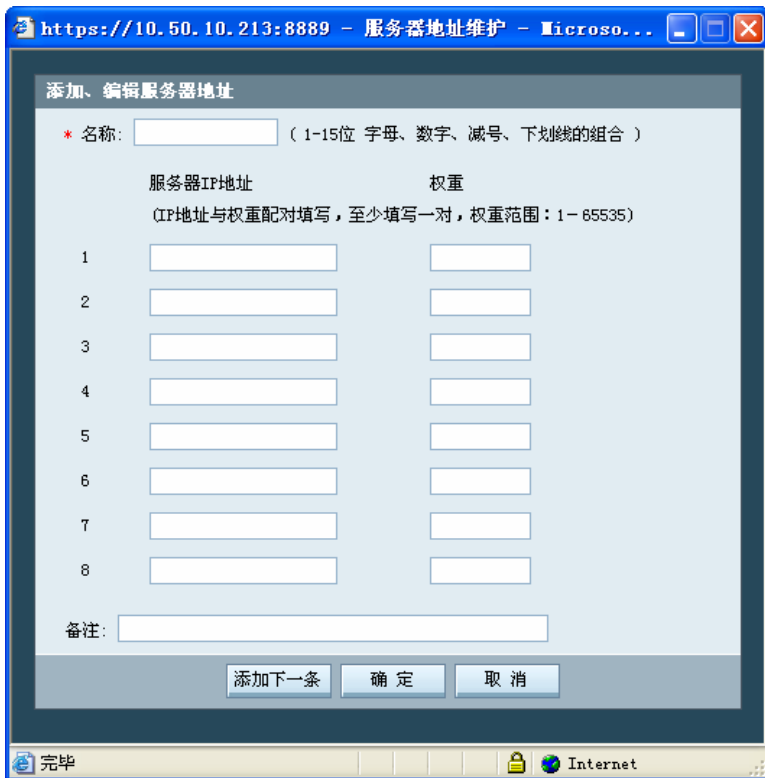
>>高级选项

*公开地址
映射为: 下拉菜单
IP地址:

中，使用的 将用到这里定义的“服务器地址”。
主要用于反向 NAT（端口映射、IP 映射）中对受保护的服务器的负载均衡。

序号	名称	备注	操作
1	svcaddr1	WEB服务器组	
2	svcaddr2	Mail服务器组	

在“对象定义>>地址>>服务器地址”界面中，点击 ，将弹出以下界面：







值 域	说 明
-----	-----

服务器 IP 地址	多台服务器对外提供同一服务时，建议将这多个 IP 地址写在服务器地址中。 每种服务最多可同时支持 8 个 IP 地址（服务器）。
权重	多台服务器对外提供同一服务时，根据这里设置的权重实现访问流量的负载均衡。 权重必须和 IP 地址一一对应。 数字越大，则权重越高。 例：服务器 A（IP 地址：192.168.22.23）权重为 60，服务器 B（IP 地址：192.168.22.24）权重为 20，则服务器 A 接受到的流量为服务器 B 接受流量的 3 倍。

8.2.4.地址>>NAT 地址池

在“安全策略>>安全规则”的 NAT、IP 映射和端口映射规则中，使用的

* 源地址转换为： 将用到这里定义的“NAT 地址池”。

序号	名称	地址	备注	操作
1	nataddr1	192.168.10.123 / 255.255.255.255		 
2	nataddr2	192.168.11.123 / 255.255.255.255		 

在“对象定义>>地址>>NAT 地址池列表”界面中，点击 ，将弹出以下界面：



值 域	说 明
名称	NAT 地址的名称，必须满足：1-20 位字母、数字、减号、下划线组合。
地址	<p>IP 地址。</p> <p>两种添加 IP 地址的方式：</p> <p>（1）IP/MASK 方式：自动应用 IP 和掩码运算来表示一个网段。例如：输入 192.168.10.123/255.255.255.0，则添加成功后变为 192.158.25.0/255.255.255.0。</p> <p>如果希望指定一台主机，请选择掩码为 255.255.255.255。</p> <p>（2）IP1-IP2 方式：IP1 必须小于或等于 IP2。如果只指定一台主机，可以让 IP1 和 IP2 相等。</p>
备注	备注为可选项。备注中可以输入任何字符，但是必须小于等于 255 个字节，即 255 个英文字符或者 127 个汉字。



- (1) 一个 NAT 地址池最多支持 254 个 IP 地址。
- (2) 所有 NAT 地址池中不同 IP 地址的总数不超过 4096 个。
- (3) IP 地址不能跨网段。

8.3. 服务

服务用于：

- (1) “安全策略”下的：代理规则、包过滤规则、NAT 规则、端口映射规则
- (2) “用户认证”下的：用户、用户组


在“对象定义>>服务”中，定义了三种服务：


- (a) 基本服务：可以“协议 + 源端口 + 目的端口”。
 - (b) ICMP 服务：可指定 type 和 code。
 - (c) 动态服务：目前支持 H323、SIP、FTP、SQLNET 四种动态协议。
- (3) 服务组：上述三种服务的任意组合。

8.3.1. 服务>>服务列表

序号	服务名	协议	备注	操作
1	ah	协议号 51	加密协议	 
2	dhcp	UDP (67, 68) - (67, 67)	dhcp & bootp	 
3	dns	TCP (0, 65535) - (53, 53) UDP (0, 65535) - (53, 53)	域名解析服务	 
4	esp	协议号 50	IP加密认证协议	 
5	gre	协议号 47	封装协议	 
6	http	TCP (0, 65535) - (80, 80)	www服务	 
7	https	TCP (0, 65535) - (443, 443)	https服务	 
8	ike	UDP (0, 65535) - (500, 500) UDP (0, 65535) - (4500, 4500)	Internet密钥交换协议	 
9	l2tp	UDP (0, 65535) - (1701, 1701)	第二层隧道协议	 
10	lotusnote	TCP (0, 65535) - (1352, 1352) UDP (0, 65535) - (1352, 1352)	Lotus notes	 
11	netbios	TCP (0, 65535) - (137, 137) TCP (0, 65535) - (139, 139) UDP (0, 65535) - (137, 137) UDP (0, 65535) - (138, 138)	windows文件共享	 
12	ntp	UDP (0, 65535) - (123, 123)	时间服务器服务	 
13	oicqc	UDP (0, 65535) - (4000, 4000)	QQ客户端打开端口	 
14	oicqs	UDP (0, 65535) - (8000, 8000)	QQ服务器打开端口	 
15	pcanywhere	TCP (0, 65535) - (5631, 5632) UDP (0, 65535) - (5631, 5632)	pcanywhere	 
16	pop3	TCP (0, 65535) - (110, 110)	邮件接收服务	 
17	pptp	TCP (0, 65535) - (1723, 1723) 协议号 47	点对点隧道协议	 
18	secgate_auth	TCP (0, 65535) - (9998, 9998) UDP (0, 65535) - (9998, 9998)	SecGate防火墙用户认证	 
19	secgate_global	TCP (0, 65535) - (161, 161) UDP (0, 65535) - (161, 161)	SecGate防火墙集中管理	 
20	secgate_ha_conf	TCP (0, 65535) - (9223, 9223) UDP (0, 65535) - (9455, 9455)	SecGate防火墙HA功能配置同步服务	 
21	secgate_https	TCP (0, 65535) - (8889, 8889) TCP (0, 65535) - (8888, 8888)	SecGate防火墙WEB管理	 
22	smtp	TCP (0, 65535) - (25, 25)	邮件发送服务	 
23	snmp	UDP (0, 65535) - (161, 161)	简单网络管理协议	 



在标题和列表之间，最左侧有一个下拉框（如图所示：）点击以后，列表中 will 只显示出属于该类的所有服务。在此下拉框中，选中不同类型的服务，点击

，弹出的界面略有不同。

选中 ，点击 ，将弹出以下界面：



可以看到，“动态服务”和“ICMP”均已置灰，只能在“基本服务”中添加：

值 域	说 明
协议	可以设置 TCP、UDP 和指定协议号（非 TCP、非 UDP 协议）。 TCP 和 UDP 协议必须指定端口，低端口和高端口必须成对出现，若低端口和高端口都没出现，则默认为 0-65535，表示所

	<p>有端口。</p> <p>选择指定协议号时,若该协议有端口的概念,则与 TCP 和 UDP 指定端口的用法相同;若该协议无端口的概念,则无需填写源端口和目的端口。</p>
源端口	<p>指定访问该服务的源主机 IP 地址所使用的端口</p> <p>从低端口到高端口的一段地址范围,如果只想表示一个端口,则把低端口和高端口设成相同。</p> <p>低端口小于等于高端口</p> <p>端口的取值范围为 0 到 65535</p> <p>源端口通常设为 0-65535,表示所有端口</p>
目的端口	<p>指定提供该服务 IP 地址所使用的端口</p> <p>从低端口到高端口的一段地址范围,如果只想表示一个端口,则把低端口和高端口设成相同的数字。</p> <p>低端口小于等于高端口</p> <p>端口的取值范围为 0 到 65535</p> <p>目的端口通常是有限的一个或者几个端口,例如:低 80 高 80</p>



- (1) 一个基本服务最少需要 1 对“协议+源端口+目的端口”,最多同时支持 8 对。通常只填写 1 对,应该首选填写序号小的。
- (2) 通常情况下,源端口不需要填写,除非是一些特定的应用使用固定的端口才需要填写。

选中 **动态**，点击 **添加**，将弹出以下界面：



可以看到，“ICMP”和“基本服务”均已置灰，只能在“动态服务”中添加：

值 域	说 明
协议	目前支持 H323、SQLNET、FTP、SIP 四种动态协议。
端口	为第一个连接使用的端口，默认的为：

	H323	1720
	SQLNET	1521
	FTP	21
	SIP	5060
管理员可以根据需求修改上述协议的默认端口。		

选中 ，点击 ，将弹出以下界面：



可以看到，“动态服务”和“基本服务”均已置灰，只能在“ICMP”中添加：

值域	说明
类型 (type)	ICMP 协议的 type 类型
代码 (code)	ICMP 协议的 code 代码

8.3.2. 服务>>服务组

序号	名称	成员	备注	操作
1	svcgrp1	ftp h323 icmp		 
2	svcgrp2	https http		 

服务组用于“安全策略>>安全规则”和“用户认证>>用户组”。





服务组的成员可以是“对象定义>>服务>>服务列表”中已经定义过的基本服务、动态服务和 ICMP 服务。

在“对象定义>>服务>>服务组”界面中，点击 ，将弹出以下界面：



值 域	说 明
服务列表	列出所有在“对象定义>>服务>>服务列表”中定义的所有服务，包括“基本服务”、“动态服务”和“ICMP”。 被添加到服务组成员列表中的服务将不再显示于服务列表中。
服务组成员	列出本组的所有成员。 服务组至少要有一个成员。

提供以下操作：

操作功能	说 明
	添加成员，点击  把选中的服务添加到成员列表中。
	删除成员，点击  把选中的成员移回到服务列表中。

8.4. 代理

应用代理工作在应用层，针对 TCP 协议下的应用（HTTP、FTP、TELNET、SMTP、POP3）提供过滤。代理的安全性高，性能相对低。

代理用于：“安全策略>>安全规则”中的“代理规则”中。


在“对象定义>>代理”中，定义两类代理：


（1）预定义代理：包括应用代理（HTTP 代理、FTP 代理、TELNET 代理、SMTP 代理、POP3 代理）

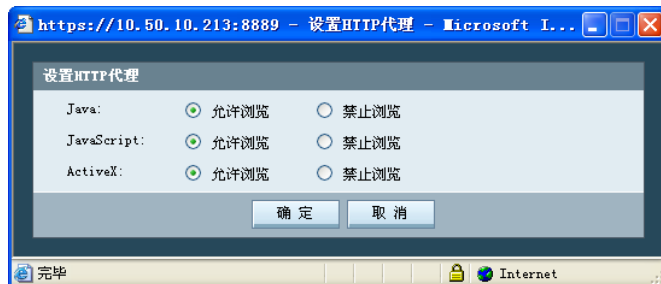
(2) 自定义代理：管理员自己指定的应用代理。目前只支持 TCP 协议。

8.4.1.代理>>预定义代理


预定义代理	端口号	高级设置
HTTP代理	端口: <input type="text" value="80"/>	
FTP代理	端口: <input type="text" value="21"/>	
TELNET代理	端口: <input type="text" value="23"/>	
SMTP代理	端口: <input type="text" value="25"/> 内容过滤	
POP3代理	端口: <input type="text" value="110"/> 内容过滤	

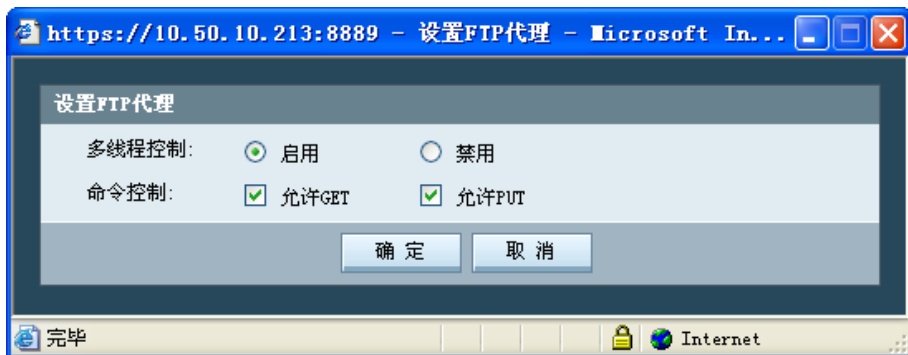
值 域	说 明
预定义代理	预定义代理包括 HTTP 代理、FTP 代理、TELNET 代理、SMTP 代理、POP3 代理。
端口号	设置对应代理的端口号
高级设置	编辑  对应代理的设置

点击 HTTP 代理对应 ，弹出以下界面：




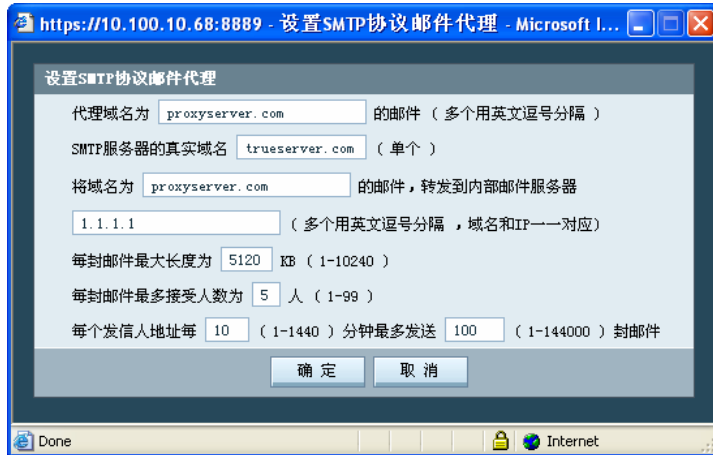
值 域	说 明
Java	允许浏览：不过滤 Java 代码 禁止浏览：对 Java 代码进行过滤
JavaScript	允许浏览：不过滤 JavaScript 代码 禁止浏览：对 JavaScript 代码进行过滤
ActiveX	允许浏览：不过滤 ActiveX 代码 禁止浏览：对 ActiveX 代码进行过滤

点击 FTP 代理对应, 弹出以下界面:




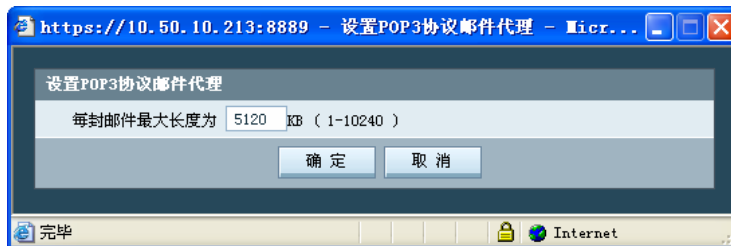
值 域	说 明
多线程控制	启用：不过滤多线程命令 禁用：过滤多线程命令
命令控制	允许 GET：不过滤 get 命令 允许 PUT：不过滤 put 命令

点击 SMTP 代理对应, 弹出以下界面:



在这个页面上可以设置需要代理的邮件域名、SMTP 服务器的真实域名、内部邮件服务器的 IP 地址等。

点击 POP3 代理对应 ，弹出以下界面：



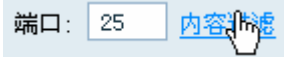
POP3 能够对邮件大小限制，并按关键字对邮件主题、附件名过滤。



- (1) 各代理设置的端口（如：TELNET代理 端口：）均为该代理的工作端口，即该代理在该端口监听。该页面中的所有代理都只能连接远程标准服务，即远程服务器的服务端口均是标准的，不能是定制的。例如，FTP 代理只能连接监听 21 端口的外部 ftp 服务器，不能连接监听所有非 21 端口的 FTP 服务器。

- (2) FTP 代理中，禁止 get 时，安全网关不会显示 ftp 服务器上的文件列表；禁止 put 时，安全网关会将一个 0 字节的文件放在 ftp 服务器上。
- (3) 如果需要在客户端进行域名解析，则必须先“安全策略>>安全规则”中添加一条允许相应 DNS 服务（UDP 协议，目的端口为 53）的安全规则，客户端才能穿过安全网关和服务器通信。

设置 SMTP 代理内容过滤

点击“SMTP 代理”一栏的“内容过滤”链接（如图：），将弹出以下窗口

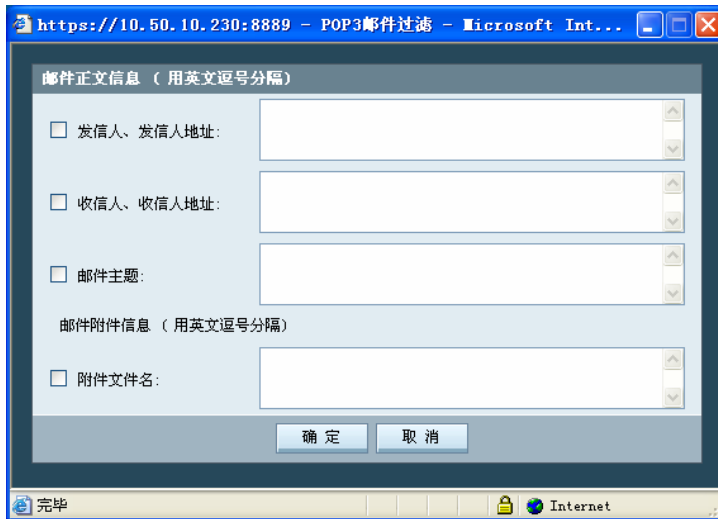



值 域	说 明
复选框 <input type="checkbox"/>	表示是否启用该项检查。

关键字	每个关键字长度最多为 255 个字符。最多可输入 2048 个字符。 用英文逗号分隔。
-----	--

设置 POP3 代理内容过滤

点击“POP3 代理”一栏的“内容过滤”链接（如图：[端口：110](#) [内容过滤](#)），
将弹出以下窗口



值 域	说 明
复选框 	表示是否启用该项检查。
关键字	每个关键字长度最多为 255 个字符。最多可输入 2048 个字符。 用英文逗号分隔。 启用该项检查以后，必须设置关键字。

8.4.2.代理>>自定义代理

序号	名称	端口	备注	操作
1	proxy1	80		 
2	proxy2	8080		 

目前只支持 TCP 协议的代理。

在“对象定义>>代理>>自定义代理”界面中，点击 ，将弹出以下界面：

添加、编辑自定义代理

* 名称: (1-15位 字母、数字、减号、下划线的组合)

* 端口: (TCP协议)

备注:

值 域	说 明
名称	代理名称，必须是 1-20 位字母、数字、减号、下划线的组合
端口	范围为：1—65535

8.5. 时间

很多访问控制和时间有紧密的关系。比如，上班时间不能上网浏览新闻，但是，下班时间可以。这样，就需要有时间调度策略。

在“对象定义>>时间”中，定义了两类时间：（1）一次性调度（2）周循环调度





时间组：上述类型的时间的组合

定义的时间和时间组在以下几处用到：

(1) 安全规则：包过滤规则、NAT 规则、IP 映射规则、端口映射规则、代理规则。

(2) 本地用户认证：用户、用户组的安全策略和可使用服务。

8.5.1.时间>>时间列表

序号	名称	备注	操作
1	work_time	工作时间	 
2	rest_time	假期	 

可以按照两种方式来定义时间：

- (1) 一次性调度
- (2) 周循环调度

在“对象定义>>时间”界面中，点击 ，将弹出以下界面：

添加、编辑时间列表

* 名称: (1-15位 字母、数字、减号、下划线的组合)

一次性调度 有效时间格式 (YYYY/MM/DD hh:mm:ss)

起始时间: 终止时间:

周循环调度

调度日期	起始时间 有效时间格式 (hh:mm:ss)	终止时间 有效时间格式 (hh:mm:ss)
星期日	<input type="text"/>	<input type="text"/>
星期一	<input type="text"/>	<input type="text"/>
星期二	<input type="text"/>	<input type="text"/>
星期三	<input type="text"/>	<input type="text"/>
星期四	<input type="text"/>	<input type="text"/>
星期五	<input type="text"/>	<input type="text"/>
星期六	<input type="text"/>	<input type="text"/>

备注:

值 域	说 明
一次性调度	指定起始和终止年月日、时分秒 例如: 2005/10/01 00:00:00 至 2005/10/07 23:59:59 为放假时间, 禁止所有内部主机访问外部。则在时间定义中定义一条一次性时间, 再到安全规则中定义相应的规则即可。
周循环调度	每周七天, 每天都可以指定起始时间和终止时间, 指定时分秒。

例如：需要实现这样的功能：在工作时间禁止所有 WEB 浏览。则设置一条禁止的安全规则，源地址和目的地址均设为“any”，服务选择“HTTP”，时间段选择上图设置的“worktime”，其它各项使用默认值即可。



当和“用户认证”功能结合使用时，有可能观察到 2-4 秒的延迟，不和“用户认证”结合使用则没有这段延迟。这是因为“用户认证”功能的调度和响应需要 2-4 秒的时间。

8.5.2.时间>>时间组

序号	名称	时间组成员	备注	操作
1	timegrp1	work_time		 
2	timegrp2	rest_time		 

在“对象定义>>时间>>时间组”界面中，点击 ，将弹出以下界面：

添加、编辑时间组

* 名称: (1-15位 字母、数字、减号、下划线的组合)

时间列表成员

时间组成员

备注:

值 域	说 明
时间列表成员	列出所有在“对象定义>>时间>>时间列表”中定义的时间。 被添加到时间组成员列表中的时间将不再显示于时间列表中。
时间组成员	该时间组的所有成员。

提供以下操作：

操作功能	说明
<input style="border: 1px solid gray;" type="button" value=" >> "/>	添加成员，点击 <input style="border: 1px solid gray;" type="button" value=" >> "/> 把选中的时间添加到成员列表。
<input style="border: 1px solid gray;" type="button" value=" << "/>	删除成员，点击 <input style="border: 1px solid gray;" type="button" value=" << "/> 把选中的成员移回到时间列表中。

8.6. 带宽列表





网络带宽资源是非常宝贵的。为了保证高效的使用带宽，限制对带宽的滥用，优

先保障重要服务，有必要进行带宽控制。SecGate 3600-G10 安全网关通过保证带宽和限制带宽来保证带宽的高效使用。

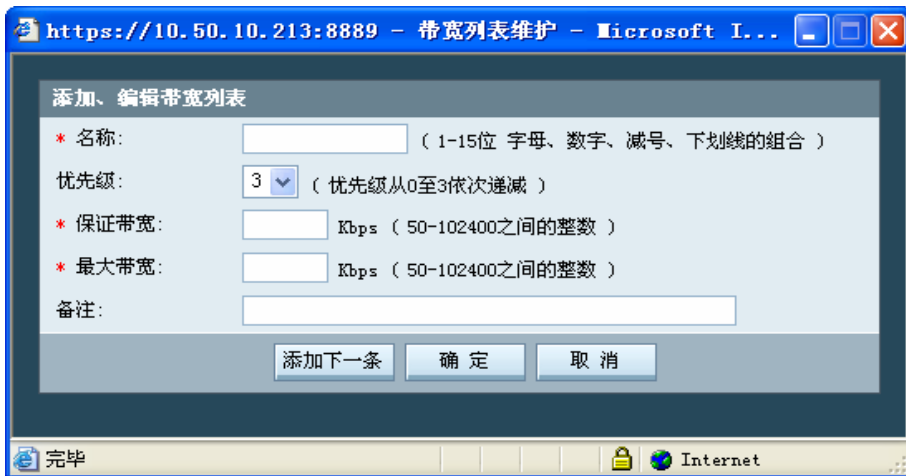
在“对象定义>>带宽列表”中可以按优先级、保证带宽和最大带宽来定义带宽控制策略。

定义的所有带宽策略在“安全策略>>安全规则”中的“流量控制”（如图所示：

流量控制:) 用到。

序号	名称	优先级	保证带宽(Kbps)	最大带宽(Kbps)	备注	操作
1	band1	3	50	100		 
2	band2	3	1000	8000		 

在“对象定义>>带宽列表”界面中，点击 按钮，将弹出以下界面：

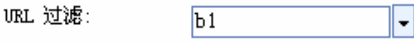


值 域	说 明
优先级	当各项服务竞争带宽资源时，总是首先保障优先级高的服务。

	未启用带宽控制的规则，默认优先级为 3。 对优先级相同时，均分可以使用的带宽，但最大不超过各策略的最大带宽。
保证带宽	任何情况下，应用该带宽控制策略的规则，可以保证至少使用的带宽不少于此处指定的带宽值。
最大带宽	应用该带宽控制策略的规则，可以抢占可能使用的带宽资源，但不应该超过此处指定的带宽值。

8.7. URL 列表

WEB 服务是互联网上使用最多的服务之一。互联网上信息鱼龙混杂，有部分不良信息，因此必须对其访问进行必要的控制。SecGate 3600-G10 安全网关可以通过对某些 URL 进行过滤实现对访问不良信息的控制。通过使用黑名单和白名单来控制用户不能访问哪些 URL，可以访问哪些 URL。

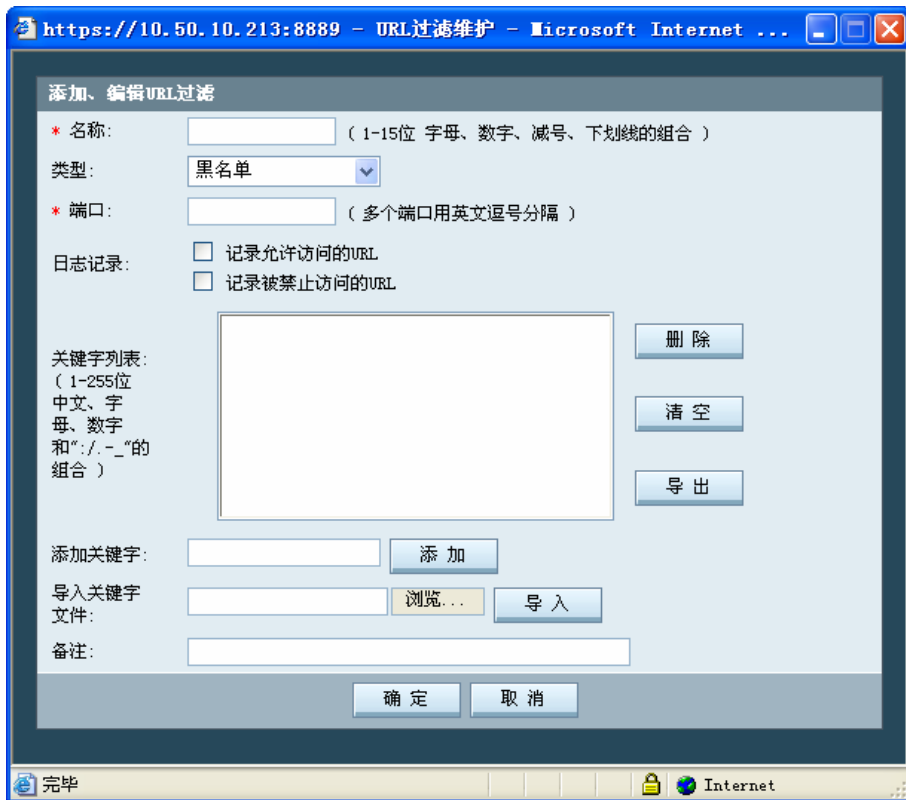
在“安全策略>>安全规则”中配置包过滤、NAT 策略均可以针对 HTTP 协议进行 URL 过滤（如图所示：），URL 过滤所使用的列表就是这里定义的 URL 列表。

URL 过滤提供两种类型的 URL 列表：


- (1) 黑名单：禁止名单中的 URL 通过，其它的 URL 均可访问。
- (2) 白名单：只允许名单中的 URL 通过，其它的 URL 均不允许访问。

序号	名称	类型	备注	操作
1	b1	黑名单	黑名单	 
2	w1	白名单	白名单	 


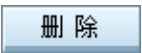

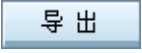

在“对象定义>>URL 列表”界面中，点击 ，将弹出以下界面：




值 域	说 明
类型	黑名单：禁止名单中的 URL 通过，其它的 URL 均可访问。 白名单：只允许名单中的 URL 通过，其它的 URL 均不允许访问。

端口	对基于 HTTP 协议的访问，如果目的端口为此处指定的端口，则该数据包将接受安全网关的 URL 过滤检查。  不能对基于 HTTPS 协议的访问进行 URL 过滤，该访问通过 SSL 协议进行了加密。
日志记录	当数据包接受 URL 过滤时，是否记录允许访问和禁止访问的 URL。
关键字列表	URL 关键字列表 每个关键字为 1—255 位字母、数字、和“:/-”的组合。

为便于添加、修改、删除关键字，提供了以下操作：

操作功能	说 明
	把关键字添加到关键字列表中
	删除关键字列表中选定的关键字
	删除关键字列表中的所有内容
	到关键字列表导出成一个文本文件，每行一个关键字
	把文本文件 (*.txt) 导入到关键字列表中，文件格式为每行一个关键字

 修改 URL 列表对象以后，需要到“安全策略>>安全规则”界面点击“刷新”按钮，修改才能生效。

9. 安全策略

安全策略是安全网关的核心功能。安全网关所有的访问控制均根据安全规则的设置完成。

安全规则包括：

- (1) 包过滤规则
- (2) NAT 规则（网络地址转换）
- (3) IP 映射规则
- (4) 端口映射规则
- (5) 代理规则

9.1. 安全策略>>安全规则

安全网关的基本策略：没有明确被允许的行为都是被禁止的。

根据管理员定义的安全规则完成数据帧的访问控制，规则策略包括：“允许通过”、“禁止通过”、“NAT 方式通过”、“IP 映射方式通过”、“端口映射方式通过”、“代理方式通过”、“病毒过滤方式通过”。支持对源 IP 地址、目的 IP 地址、源端口、目的端口、服务、流入网口、流出网口等控制。

另外，根据管理员定义的基于角色控制的用户策略，并与安全规则策略配合完成访问控制，包括限制用户在什么时间、什么源 IP 地址可以登录安全网关系统，该用户通过认证后能够享有的服务。

SecGate 3600-G10 安全网关提供基于对象定义的安全策略配置。对象包括地址和地址组、NAT 地址池、服务器地址、服务（源端口、目的端口、协议）和服务组、时间和时间组、用户和用户组（包括用户策略：如登录时间与地点，源 IP/目的 IP、目的端口、协议等）、连接限制（保护主机、保护服务、限制主机、限制服务）带宽策略（最大带宽、保证带宽、优先级）、URL 过滤策略。最大限度提供方便性与灵活性。



安全网关按顺序匹配规则列表：按顺序进行规则匹配，按第一条匹配上的规则执行，不再匹配该条规则以下的规则。





序号	规则名	源地址	目的地址	服务	类型	选项	操作
1	p1	DMZ	Trust	dhcp	允许		



系统不对规则进行逻辑性检查，需要由管理员自己判定以保证规则符合逻辑。例如，即使有两条矛盾的安全规则并存，系统也不警告报错。

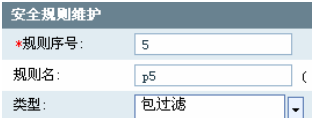
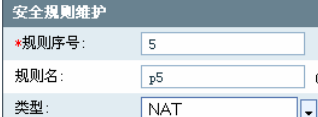
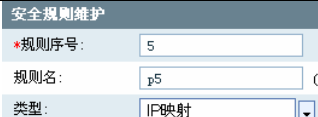
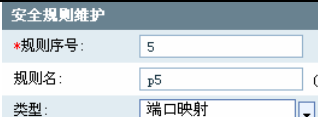
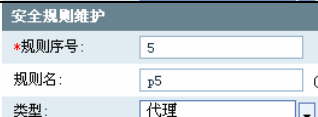


图标说明：

域 名	说 明
	包过滤规则，允许访问
	包过滤规则，禁止访问

	策略 VPN 功能
	具有记录日志功能
	具有流量控制功能
	具有时间调度功能
	具有用户认证功能
	具有连接数限制功能
	具有 P2P 限制功能
	具有 URL 过滤功能
	生效状态 如果点击该图标，则改变该条规则状态，即变成无效状态
	无效状态 如果点击该图标，则改变该条规则状态，即变成生效状态
<div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> 序号 </div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> <input type="checkbox"/> 1 </div> <div style="color: red; font-weight: bold; font-size: 1.2em; margin-bottom: 10px;">  </div> <ul style="list-style-type: none"> ● 可以“删除”多条选中的规则 ● 点击“生效”按钮，把所有选中的规则生效状态置反，即生效的规则变成不生效的规则，不生效的规则变成生效的规则 	<p>选中复选框，可以和按钮（如图所示：</p> <div style="border: 1px solid gray; padding: 5px; text-align: center; margin: 5px 0;"> 编辑 复制 删除 移动 生效 刷新 </div> <p>）配合，进行相应动作。</p>

- 只能“编辑”“复制”“移动”一条规则

功能说明：

域 名	说 明
	添加包过滤规则
	添加 NAT 规则
	添加 IP 映射规则
	添加端口映射规则
	添加代理规则
	编辑选中的规则 一次只能编辑一条规则
	复制选中的规则，一次只能复制一条规则 为更高效地添加安全规则，提供了“复制”按钮。 操作步骤： 1. 选中希望复制的规则（只能选中一条）

	<ol style="list-style-type: none"> 2. 点击“复制”按钮 3. 弹出该条规则对应的窗口。默认序号为当前最大序号加 1，其它各项与选中的规则相同 4. 修改相应的数据项（序号也可以修改） 5. 点击“确定”即可
<div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 0 auto;">删除</div>	删除选中的规则，可同时删除多条规则
<div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 0 auto;">移动</div>	<p>移动规则，一次只能移动一条规则</p> <p>规则的顺序非常重要，有时，需要把一条现有的规则移到更合适的位置，因此提供了“移动”按钮。</p> <p>操作步骤：</p> <ol style="list-style-type: none"> 1. 选中希望移动的规则（只能选中一条） 2. 点击“移动”按钮 3. 弹出移动对话框，如图所示： <div data-bbox="518 1090 1171 1242" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center; background-color: #4f81bd; color: white; padding: 2px;">安全规则移动</p> <p style="text-align: center;">第3条规则移动到：</p> <p style="text-align: center;"> <input checked="" type="radio"/> 第 <input style="width: 30px;" type="text"/> 条之前 <input type="radio"/> 第 <input style="width: 30px;" type="text"/> 条之后 </p> <p style="text-align: center;"> <input type="button" value="确定"/> <input type="button" value="取消"/> </p> </div> 4. 填入希望移到的位置 5. 点击“确定”即可 <p>注意 1. 如果希望移动到的位置大于当前最大序号，则移动到最后。</p>

	<p>2. 规则移动以后，其它规则相应调整位置，以保证规则的顺序和连续。</p>
<p></p>	<p>改变规则的状态，即把无效的规则变为生效的规则，把生效的规则变成无效的规则。</p> <p>可同时改变多条规则的生效状态。</p> <p>操作步骤：</p> <ol style="list-style-type: none"> 1. 选中希望改变状态的规则（可选中多条）。 2. 点击“生效”按钮。 3. 会把所有选中的规则生效状态置反，即生效的规则变成不生效的规则，不生效的规则变成生效的规则。 <p> 该按钮同时具备生效->无效，无效->生效的功能。</p>
<p></p>	<p>使所有规则重新生效。</p> <p>当被引用的对象被修改以后，或者添加修改删除了 URL 列表后，需要点击该按钮，使所有规则重新生效。</p> <p>操作步骤： 直接点击该按钮即可</p>
<p><input type="checkbox"/> 全选</p>	<p>点击以后，选中本页中所有规则</p>

跳转到 全部 <ul style="list-style-type: none"> N A T 规则列表 端口映射规则列表 IP 映射规则列表 包过滤规则列表 代理规则列表 <li style="background-color: #0056b3; color: white; padding: 2px;">全部 	点击以后，筛选出所选类型的安全规则，其它类型的规则被过滤掉。
--	--------------------------------

分页显示工具条，如下图所示：



详细说明请参见本手册的“对象定义通用功能介绍”。

数据域说明：

域 名	说 明
序号	已定义规则的序号，表示规则的先后顺序。 点击表头的 序号 ，可按升序降序对规则进行排序。
规则名	已定义规则的名称 点击表头的 规则名 ，可按升序降序对规则进行排序。
源地址	规则的源地址
目的地址	规则的目的地地址
服务	规则的服务
类型	安全规则的访问控制类型，包括： <ul style="list-style-type: none"> (1) 包过滤规则 禁止  (2) 包过滤规则 允许  (3) NAT 规则（网络地址转换）

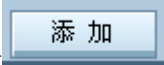
	(4) IP 映射规则 (5) 端口映射规则 (6) 代理规则
选项	安全规则的其他项功能，依次为： 用户认证  ，日志记录  、流量控制  ，时间控制  、连接限制  、P2P 限制  、URL 过滤  、若对应的位置为不出现以上图标，则表示无该项功能。
生效	 表示该规则为生效状态，点击  以后该条规则变成无效状态   表示该规则为无效状态，点击  以后该条规则变成生效状态 

9.1.1.包过滤规则

提供基于状态检测（基于 TCP/UDP/ICMP 协议）的动态的包过滤。

包过滤规则可以实现对源地址/掩码、目的地址/掩码、服务、流入流出网口的访问控制，可以设置对这类经过安全网关的数据包是允许还是禁止。另外，是否启用用户认证、是否启用带宽控制、是否启用 URL 过滤、是否启用连接限制功能以及是否记录日志，是否走 VPN 隧道都在包过滤规则中设置。包过滤规则是管理员应用最多的安全规则。SecGate 3600-G10 安全网关的包过滤规则功能十分灵活、强大。

支持的协议包括基本协议（如 http、telnet、smtp 等）、ICMP、动态协议（如 h323、ftp、sip、sqlnet 等）。

在“安全策略>>安全规则”界面中，点击 ，将弹出以下界面：



安全规则维护

*规则序号:

规则名: (1-15位 字母、数字、减号、下划线的组合)

类型:

条件

源地址: IP地址 掩码

目的地址: IP地址 掩码

服务:

操作

动作: 允许 禁止 日志记录:

<<高级选项

时间调度: 流量控制:

检查流 入网口: 检查流 出网口:

用户认证:

深度行为检测

连接限制: 保护主机 保护服务 限制主机 限制服务

P2P限制: URL 过滤:

域 名	说 明
序号	输入新增策略规则的序号。 安全网关按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。 若该数字与已定义的规则序号有重复，则安全网关会自动将原策略规则以及序号排在之后的所有规则自动后移一个数字，将新增策略规则

	<p>的序号设为输入的序号。</p> <p>若不修改界面中序号，即为添加到最后。</p> <p>如果序号大于已有规则总数加 1，即为添加到最后。</p>
规则名	<p>安全规则的名称。</p> <p>规则名必须是 1—15 位字母、数字、减号、下划线的组合。</p> <p>规则名可以重复。</p> <p>默认规则名为“pf”+ 默认序号。</p> <p>如果把规则名置空，则使用默认规则名“pf”</p>
源地址	<p>可选内容包括：“对象定义>>地址>>地址列表”和“对象定义>>地址>>地址组”中定义的所有对象，及“手工输入”。</p> <p>当选择“手工输入”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。</p> <p>默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0。</p>
目的地址	内容同源地址
动作	匹配到本条安全规则的数据包可以执行两种过滤策略：“允许”、“禁止”
服务	<p>可选内容包括：any，在“对象定义>>服务>>服务列表”中配置的基本服务、ICMP 服务、动态服务，以及“对象定义>>服务>>服务组”。</p> <p>默认值为 any，表示源端口任意、目的端口任意、协议任意。</p>
流入网口	强制要求符合本条规则的数据包只能从指定的网口接收。通过检查网口，可以防止 IP 欺骗。

	<p>可选内容包括：any 和所有已激活的网口。</p> <p>默认值为 any，表示不限制接收网口。</p>
流出网口	<p>强制要求符合本条规则的数据包只能从指定的网口发送。通过检查网口，可以防止 IP 欺骗。</p> <p>可选内容包括：any 和所有已激活的网口。</p> <p>默认值为 any，表示不限制接收网口。</p>
时间控制	<p>生效的安全规则将在指定的时间段内为生效状态且在其它时间段为失效状态，可选内容包括：“对象定义>>时间>>时间列表”和“对象定义>>时间组”中定义的所有对象。</p>
流量控制	<p>生效的安全规则将根据流量策略定义的优先级、保证带宽、最大带宽控制数据包的通信，可选内容包括：“对象定义>>带宽列表”中定义的所有对象。</p>
用户认证	<p>生效的安全规则（策略为“允许”）必须经过用户身份认证，在认证成功后才能有效。</p> <p>可使用的是本地帐号服务器或 radius 服务器中的用户帐号。参考“用户认证>>服务器”界面中用户认证服务器的设置。</p> <p>如果使用本地帐号服务器，可以配置用户策略，如限制用户在什么时间、什么源 IP 地址可以登录安全网关系统，该用户通过认证后能够享有的服务。参考“用户认证>>用户列表”和“用户认证>>用户组”界面中本地用户库在中设置。</p>

日志记录	设置被“允许”、“禁止”的数据包是否需要记录日志
URL 过滤	生效的安全规则（策略只能为“允许”）执行 URL 过滤，非 HTTP 协议的数据包都被放过，HTTP 协议的数据包根据这里指定的 URL 过滤规则进行关键字检查，以决定是否允许通过。 可选内容包括：“对象定义>>URL 列表”中已定义的所有 URL 对象。
保护主机	在对象定义中定义相应的连接限制，此处选上，就可以启用保护主机类别的连接限制。保护主机是限制的对服务器的 ip 的访问。
保护服务	在对象定义中定义相应的连接限制，此处选上，就可以启用保护服务类别的连接限制。保护服务是限制的对服务器的某类服务的访问。
限制主机	在对象定义中定义相应的连接限制，此处选上，就可以启用限制主机类别的连接限制。限制主机是对源地址的限制。
限制服务	在对象定义中定义相应的连接限制，此处选上，就可以启用限制服务类别的连接限制。限制服务是是对源地址发起的某类服务的访问限制。
P2P 限制	在安全策略>>P2P 限制中定义了针对 apple、ares、bt、dc、edonkey、gnu、kazaa、soul、winmx 等 P2P 协议的过滤策略及流量控制，此处选上，就可以针对该条策略启用相应的 P2P 限制策略。


9.1.2.NAT 规则

NAT（Network Address Translation）是在 IPv4 地址日渐枯竭的情况下出现的一种技术，可将整个组织的内部 IP 都映射到一个合法 IP 上来进行 Internet 的访问，NAT

中转换前源 IP 地址和转换后源 IP 地址不同，数据进入安全网关后，安全网关将其源地址进行了转换后再将其发出，使外部看不到数据包原来的源地址。一般来说，NAT 多用于从内部网络到外部网络的访问，内部网络地址可以是保留 IP 地址。

SecGate 3600-G10 安全网关支持源地址一对一的转换，也支持源地址转换为地址池中的某一个地址。

用户可通过安全规则设定需要转换的源地址（支持网络地址范围）、源端口。此处的 NAT 指正向 NAT，正向 NAT 也是动态 NAT，通过系统提供的 NAT 地址池，支持多对多，多对一，一对多，一对一的转换关系。

在“安全策略>>安全规则”界面中，点击 ，将弹出以下界面：



安全规则维护

*规则序号:

规则名: (1-15位 字母、数字、减号、下划线的组合)

类型:

条件

源地址: IP地址 掩码

目的地址: IP地址 掩码

* 服务:

操作

*源地址转换为: 日志记录:

<<高级选项

时间调度: 流量控制:

检查流 入网口: 检查流 出网口:

用户认证:

深度行为检测

连接限制: 保护主机 保护服务 限制主机 限制服务

URL 过滤: P2P限制:

域 名	说 明
序号	<p>输入新增策略规则的序号。</p> <p>安全网关按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。</p> <p>若该数字与已定义的规则序号有重复，则安全网关会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。</p> <p>若不修改界面中序号，即为添加到最后。</p> <p>如果规则的序号大于已有规则总数，即为添加到最后。</p>
规则名	<p>安全规则的名称。</p> <p>规则名必须是 1—15 位字母、数字、减号、下划线的组合。</p> <p>规则名可以重复。</p> <p>默认规则名为“nat”+ 默认序号。</p> <p>如果把规则名置空，则使用默认规则名“nat”</p>
源地址	<p>可选内容包括：“对象定义>>地址>>地址列表”中的地址对象、“对象定义>>地址>>地址组”中的地址对象，及“手工输入”。</p> <p>当选择“手工输入”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。</p> <p>默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0。</p>
目的地址	内容同源地址

服务	<p>可选内容包括：any，“对象定义>>服务>>服务列表”中的基本服务、ICMP 服务、动态服务，以及“对象定义>>服务>>服务组”中的服务对象。</p> <p>默认值为 any，表示源端口任意、目的端口任意、协议任意。</p>
源地址转换为	<p>可选内容包括：“对象定义>>NAT 地址池”中的地址对象和“网络配置>>安全网关 IP”中的 IP 地址对象，也可以设置为 by_route，应用于转换后地址是通过 adsl 拨号获得或者 dhcp 动态获取。</p>
日志记录	<p>强制要求匹配的数据包是否需要记录日志</p>
时间调度	<p>生效的安全规则将在指定的时间段内为生效状态且在其它时间段为失效状态，可选内容包括：“对象定义>>时间>>时间列表”和“对象定义>>时间>>时间组”中定义的所有对象。</p>
流量控制	<p>生效的安全规则将根据流量策略定义的优先级、保证带宽、最大带宽控制数据包的通信，可选内容包括：“对象定义>>带宽列表”中定义的所有对象。</p>
流入网口	<p>强制要求符合本条规则的数据包只能从指定的网口接收。通过检查网口，可防止 IP 欺骗。</p> <p>可选内容包括：any 和所有已激活的网口。</p> <p>默认值为 any，表示不限制接收网口。</p>
流出网口	<p>强制要求符合本条规则的数据包只能从指定的网口发送。通过检查网口，以防止 IP 欺骗。</p>

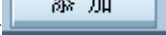
	<p>可选内容包括：any 和所有已激活的网口。</p> <p>默认值为 any，表示不限制接收网口。</p>
用户认证	<p>生效的安全规则必须经过用户身份认证，在认证成功后才能有效。</p> <p>可使用的是本地帐号服务器或 radius 服务器中的用户帐号。参考“用户认证>>服务器”界面中用户认证服务器的设置。</p> <p>如果使用本地帐号服务器，可以配置用户策略，如限制用户在什么时间、什么源 IP 地址可以登录安全网关系统，该用户通过认证后能够享有的服务。参考“用户认证>>用户列表”和“用户认证>>用户组”界面中本地用户库在中设置。</p>
保护主机	<p>在对象定义中定义相应的连接限制，此处选上，就可以启用保护主机类别的连接限制。保护主机是限制的对服务器的 ip 的访问。</p>
保护服务	<p>在对象定义中定义相应的连接限制，此处选上，就可以启用保护服务类别的连接限制。保护服务是限制的对服务器的某类服务的访问。</p>
限制主机	<p>在对象定义中定义相应的连接限制，此处选上，就可以启用限制主机类别的连接限制。限制主机是对源地址的限制。</p>
限制服务	<p>在对象定义中定义相应的连接限制，此处选上，就可以启用限制服务类别的连接限制。限制服务是是对源地址发起的某类服务的访问限制。</p>
P2P 限制	<p>在安全策略>>P2P 限制中定义了针对 apple、ares、bt、dc、edonkey、gnu、kazaa、soul、winmx 等 P2P 协议的过滤策略及流量控制，此</p>

	处选上，就可以针对该条策略启用相应的 P2P 限制策略。
URL 过滤	生效的安全规则执行 URL 过滤，非 HTTP 协议的数据包都被放过，HTTP 协议的数据包根据这里指定的 URL 过滤规则进行关键字检查，以决定是否允许通过。 可选内容包括：“对象定义>>URL 列表”中的 URL 对象。

9.1.3.IP 映射规则

IP 映射规则是将访问的目的 IP 转换为内部服务器的 IP。一般用于外部网络到内部服务器的访问，内部服务器可使用保留 IP 地址。

当管理员配置多个服务器时，就可以通过 IP 映射规则，实现对服务器访问的负载均衡。一般的应用为：假设安全网关外网卡上有一个合法 IP，内部有多个服务器同时提供服务，当将访问安全网关外网卡 IP 的访问请求转换为这一组内部服务器的 IP 地址时，访问请求就可以在这一组服务器进行均衡。

在“安全策略>>安全规则”界面中，点击 ，将弹出以下界面：

安全规则维护

*规则序号:

规则名: (1-15位 字母、数字、减号、下划线的组合)

类型:

条件

源地址: *公开地址:

IP地址: 掩 码:

操作

源地址 转换为: *公开地址 映射为:

IP地址:

日志记录:

<<高级选项

时间调度: 流量控制:

检查流 入网口: 检查流 出网口:

用户认证:

深度行为检测

连接限制: 保护主机 保护服务 限制主机 限制服务

域 名	说 明
序号	输入新增策略规则的序号。 安全网关按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。 若该数字与已定义的规则序号有重复，则安全网关会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。 若不修改界面中序号，即为添加到最后。 如果序号大于已有规则总数加 1，即为添加到最后。
规则名	安全规则的名称。

	<p>规则名必须是 1—15 位字母、数字、减号、下划线的组合。</p> <p>规则名可以重复。</p> <p>默认规则名为“vip”+ 默认序号。</p> <p>如果把规则名置空，则使用默认规则名“vip”</p>
源地址	<p>可选内容包括：“对象定义>>地址>>地址列表”中的地址对象、“对象定义>>地址>>地址组”中的地址对象，及“手工输入”。</p> <p>当选择“手工输入”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。</p> <p>默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0。</p>
公开地址	<p>用户可以访问的 IP 地址，即指定可以访问的目的 IP 地址。</p> <p>必须是单个 IP 地址，不能是网段。</p> <p>可选内容包括：“网络配置>>安全网关 IP”中的 IP 地址对象。</p>
源地址转换为	<p>可选内容包括：不转换，“对象定义>>NAT 地址池”中的地址对象、“网络配置>>安全网关 IP”中的 IP 地址对象。</p>
公开地址映射为	<p>用户实际访问的 IP 地址，即指定实际访问的目的 IP 地址。</p> <p>一般是单个 IP 地址。当是多个 IP 地址或网段时，一般用于服务器的负载均衡。</p> <p>可选内容包括：“对象定义>>地址>>地址列表”中的地址对象、“对象定义>>地址>>服务器地址”中的地址对象，及“手工输入”。</p> <p>当选择“对象定义>>地址>>服务器地址”中的地址对象，则提供服</p>

	<p>务器的负载均衡功能。参考“对象定义>>地址>>服务器地址”中的配置。</p> <p>当选择“手工输入”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。</p>
日志记录	强制要求匹配的数据包是否需要记录日志
时间调度	生效的安全规则将在指定的时间段内为生效状态且在其它时间段为失效状态，可选内容包括：“对象定义>>时间>>时间列表”和“对象定义>>时间>>时间组”中定义的所有对象。
流量控制	生效的安全规则将根据流量策略定义的优先级、保证带宽、最大带宽控制数据包的通信，可选内容包括：“对象定义>>带宽列表”中定义的所有对象。
检查流入网口	<p>强制要求符合本条规则的数据包只能从指定的网口接收。通过检查网口，可防止 IP 欺骗。</p> <p>可选内容包括：any 和所有已激活的网口。</p> <p>默认值为 any，表示不限制接收网口。</p>
检查流出网口	<p>强制要求符合本条规则的数据包只能从指定的网口发送。通过检查网口，可防止 IP 欺骗。</p> <p>可选内容包括：any 和所有已激活的网口。</p> <p>默认值为 any，表示不限制接收网口。</p>
用户认证	生效的安全规则必须经过用户身份认证，在认证成功后才能有效。


	<p>可使用的是本地帐号服务器或 radius 服务器中的用户帐号。参考“用户认证>>服务器”界面中用户认证服务器的设置。</p> <p>如果使用本地帐号服务器，可以配置用户策略，如限制用户在什么时间、什么源 IP 地址可以登录安全网系统，该用户通过认证后能够享有的服务。参考“用户认证>>用户列表”和“用户认证>>用户组”界面中本地用户库在中设置。</p>
保护主机	在对象定义中定义相应的连接限制，此处选上，就可以启用保护主机类别的连接限制。保护主机是限制的对服务器的 ip 的访问。
保护服务	在对象定义中定义相应的连接限制，此处选上，就可以启用保护服务类别的连接限制。保护服务是限制的对服务器的某类服务的访问。
限制主机	在对象定义中定义相应的连接限制，此处选上，就可以启用限制主机类别的连接限制。限制主机是对源地址的限制。
限制服务	在对象定义中定义相应的连接限制，此处选上，就可以启用限制服务类别的连接限制。限制服务是是对源地址发起的某类服务的访问限制。

9.1.4. 端口映射规则

端口映射规则是将访问的目的 IP 和目的端口转换为内部服务器的 IP 和服务端口。一般用于外部网络到内部服务器的访问，内部服务器可使用保留 IP 地址。

当管理员配置多个服务器时，都提供某一端口的服务，就可以通过配置端口映射

规则，实现对服务器此端口访问的负载均衡。一般的应用为：假设安全网关外网卡上有一个合法 IP，内部有多个服务器同时提供服务，当将访问安全网关外网卡 IP 的访问请求转换为这一组内部服务器的 IP 地址时，访问请求就可以在这一组服务器进行均衡。

在“安全策略>>安全规则”界面中，点击 ，将弹出以下界面：



安全规则维护

*规则序号: 2

规则名: p2 (1-15位 字母、数字、减号、下划线的组合)

类型: 端口映射

条件

源地址: IP地址: [] *公开地址: []

掩 码: []

* 对外服务: []

操作

源地址转换为: [] *公开地址映射为: []

IP地址: []

*对外服务映射为: [] 日志记录:

<<高级选项

时间调度: [] 流量控制: []

检查流入网口: [] 检查流出网口: []

用户认证:


深度行为检测


连接限制: 保护主机 保护服务 限制主机 限制服务

添加下一条 确定 取消

域 名	说 明
序号	输入新增策略规则的序号。 安全网关按规则序号顺序从小到大的顺序匹配规则并执行。序号为数字。 若该数字与已定义的规则序号有重复，则安全网关会自动将原策略规

	<p>则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。</p> <p>若不修改界面中序号，即为添加到最后。</p> <p>如果序号大于已有规则总数加 1，即为添加到最后。</p>
规则名	<p>安全规则的名称。</p> <p>规则名必须是 1—15 位字母、数字、减号、下划线的组合。</p> <p>规则名可以重复。</p> <p>默认规则名为“pnat”+ 默认序号。</p> <p>如果把规则名置空，则使用默认规则名“pnat”</p>
源地址	<p>可选内容包括：“对象定义>>地址>>地址列表”中的地址对象、“对象定义>>地址>>地址组”中的地址对象，及“手工输入”。</p> <p>当选择“手工输入”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。</p> <p>默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0。</p>
公开地址	<p>用户可以访问的 IP 地址，即指定可以访问的目的 IP 地址。</p> <p>必须是单个 IP 地址，不能是网段。</p> <p>可选内容包括：“网络配置>>安全网关 IP”中的 IP 地址对象。</p>
对外服务	<p>用户可以访问的服务，即指定可以访问的目的端口。</p> <p>可选内容包括：“对象定义>>服务>>服务列表”中的基本服务、ICMP 服务、动态服务的一个；不能使用服务组和 any。</p>

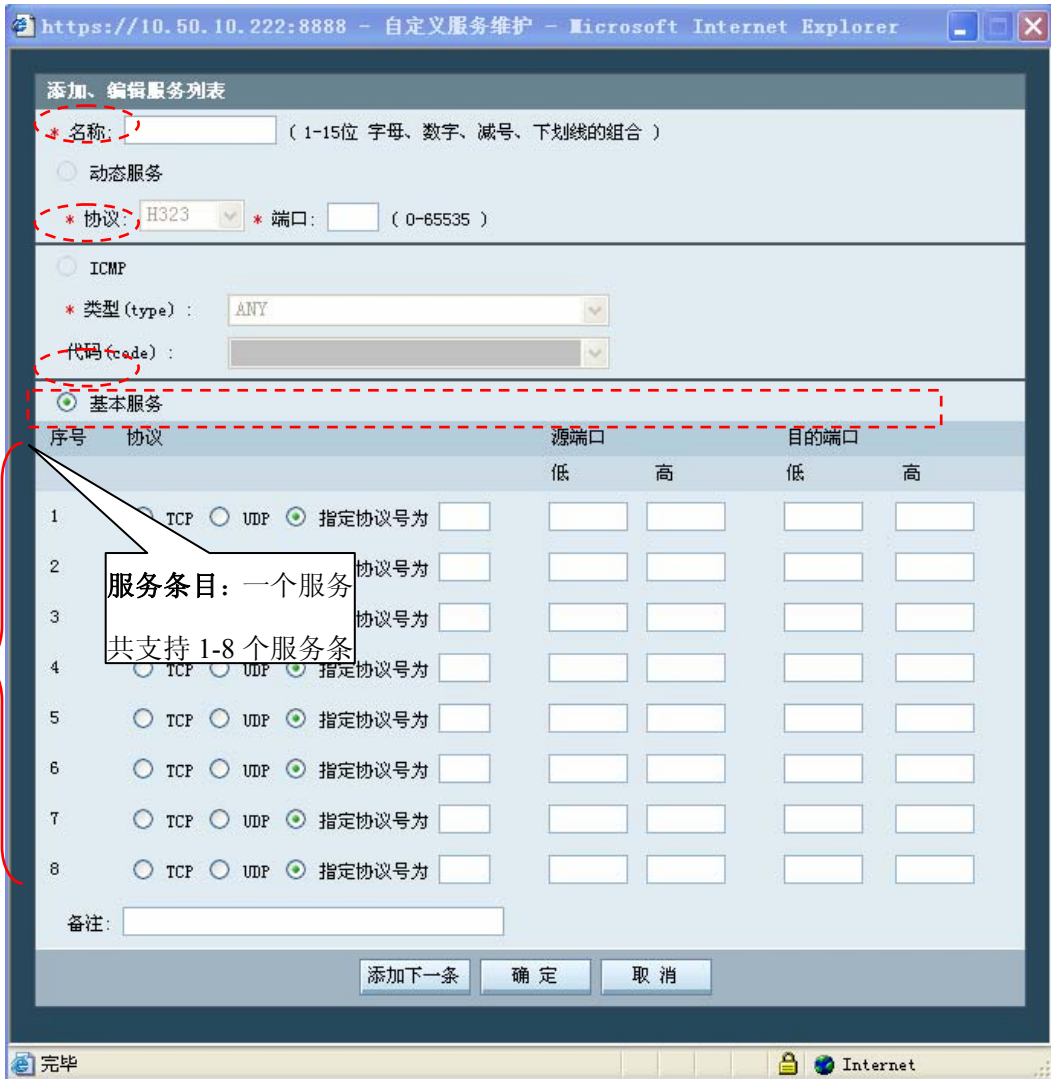
	<p>参见附表一：对外服务与内部服务选择的服务对象要严格遵守的约定。</p> <p> 所选服务的源端口和目的端口将共同作为转换的依据。</p>
源地址转换为	<p>可选内容包括：不转换，“对象定义>>NAT 地址池”中的地址对象和“网络配置>>安全网关 IP”中的 IP 地址对象。</p>
公开地址映射为	<p>用户实际访问的 IP 地址，即指定实际访问的目的 IP 地址。</p> <p>一般是单个 IP 地址。当是多个 IP 地址或网段时，一般用于服务器的负载均衡。</p> <p>可选内容包括：“对象定义>>地址>>地址列表”中的地址对象、“对象定义>>地址>>服务器地址”中的地址对象，及“手工输入”。</p> <p>当选择“对象定义>>地址>>服务器地址”中的地址对象，则提供服务器的负载均衡功能。参考“对象定义>>地址>>服务器地址”中的配置。</p> <p>当选择“手工输入”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。</p>
对外服务映射为	<p>用户可以访问的内部主机的服务，即指定可以访问的目的端口。</p> <p>可选内容包括：“对象定义>>服务>>服务列表”中的基本服务、动态服务的一个；不能使用服务组和 any。</p> <p>参见附表一：对外服务与内部服务选择的服务对象要严格遵守的约定。</p>

	 所选服务的源端口和目的端口将共同作为转换的依据。
日志记录	强制要求通过的数据包是否需要记录日志
时间调度	生效的安全规则将在指定的时间段内为生效状态且在其它时间段为失效状态，可选内容包括：“对象定义>>时间>>时间列表”和“对象定义>>时间>>时间组”中定义的所有对象。
流量控制	生效的安全规则将根据流量策略定义的优先级、保证带宽、最大带宽控制数据包的通信，可选内容包括：“对象定义>>带宽列表”中定义的所有对象。
检查流入网口	<p>强制要求符合本条规则的数据包只能从指定的网口接收。通过检查网口，可防止 IP 欺骗。</p> <p>可选内容包括：any 和所有已激活的网口。</p> <p>默认值为 any，表示不限制接收网口。</p>
检查流出网口	<p>强制要求符合本条规则的数据包只能从指定的网口发送。通过检查网口，可防止 IP 欺骗。</p> <p>可选内容包括：any 和所有已激活的网口。</p> <p>默认值为 any，表示不限制接收网口。</p>
用户认证	<p>生效的安全规则必须经过用户身份认证，在认证成功后才能有效。</p> <p>可使用的是本地帐号服务器或 radius 服务器中的用户帐号。参考“用户认证>>服务器”界面中用户认证服务器的设置。</p> <p>如果使用本地帐号服务器，可以配置用户策略，如限制用户在什么时</p>

	间、什么源 IP 地址可以登录安全网关系统，该用户通过认证后能够享有的服务。参考“用户认证>>用户列表”和“用户认证>>用户组”界面中本地用户库在中设置。
保护主机	在对象定义中定义相应的连接限制，此处选上，就可以启用保护主机类别的连接限制。保护主机是限制的对服务器的 ip 的访问。
保护服务	在对象定义中定义相应的连接限制，此处选上，就可以启用保护服务类别的连接限制。保护服务是限制的对服务器的某类服务的访问。
限制主机	在对象定义中定义相应的连接限制，此处选上，就可以启用限制主机类别的连接限制。限制主机是对源地址的限制。
限制服务	在对象定义中定义相应的连接限制，此处选上，就可以启用限制服务类别的连接限制。限制服务是是对源地址发起的某类服务的访问限制。


附表一：公开服务与内部服务选择的服务对象要严格遵守的约定（参考下图）


对象定义中的服务对象		
服 务		服务组
基本服务	协议类型必须同为 TCP 或同为 UDP	成员数量一致 每一个成员必须符合对服务的要求
	目的端口数量必须一致	
动态服务	服务条目数量必须一致	
ICMP	协议类型一致	
	不能做端口映射	



9.1.5.代理规则

支持的服务包括协议 http,telnet,smtp, pop3,ftp 和自定义 TCP 代理。

在“安全策略>>安全规则”界面中，点击 ，将弹出以下界面：



安全规则维护

*规则序号:

规则名: (1-15位 字母、数字、减号、下划线的组合)

类型:

条件

源地址: IP地址 掩码

目的地址: IP地址 掩码

*服务:

操作

*代理: 日志记录:

<<高级选项

时间调度:

域 名	说 明
序号	输入新增策略规则的序号。 安全网关按规则序号顺序从小到大的顺序匹配规则并执行，序号为数字。 若该数字与已定义的规则序号有重复，则安全网关会自动将原策略规则以及序号排在其后的所有规则自动后移一个数字，将新增策略规则的序号设为输入的序号。 若不修改界面中序号，即为添加到最后。 如果序号大于已有规则总数加 1，即为添加到最后。
规则名	安全规则的名称。

	<p>规则名必须是 1—15 位字母、数字、减号、下划线的组合。</p> <p>规则名可以重复。</p> <p>默认规则名为 “proxy” + 默认序号。</p> <p>如果把规则名置空，则使用默认规则名 “proxy”。</p>
源地址	<p>可选内容包括：“对象定义>>地址>>地址列表”和“对象定义>>地址>>地址组”中定义的所有对象，及“手工输入”。</p> <p>当选择“手工输入”，则下方的“IP 地址”和“掩码”变为可输入状态，可直接在此指定 IP 和掩码。</p> <p>默认值 IP 为 0.0.0.0，默认掩码为 0.0.0.0。</p>
目的地址	内容同源地址
服务	<p>可选内容包括：any，在“对象定义>>服务>>服务列表”中配置的基本服务、ICMP 服务、动态服务，以及“对象定义>>服务>>服务组”。</p> <p>默认值为 any，表示源端口任意、目的端口任意、协议任意。</p>
代理	<p>可选择内容包括：http 代理、ftp 代理、telnet 代理、smtp 代理、pop3 代理。各类型的代理在“对象定义>>代理>>预定义代理”或“对象定义>>代理>>自定义代理”中配置。</p> <p>默认值为 http 代理。</p>
时间调度	<p>生效的安全规则将在指定的时间段内为生效状态且在其它时间段为失效状态，可选内容包括：“对象定义>>时间>>时间列表”和“对象定义>>时间组”中定义的所有对象。</p>

9.2. 安全策略>>地址绑定

地址绑定是防止 IP 欺骗和防止盗用 IP 地址的有效手段。并且 SecGate 3600-G10 安全网关提供自动探测 IP/MAC 对功能，可以减轻管理员手工收集 IP/MAC 对的工作量。

如果安全网关某网口配置了“IP/MAC 地址绑定”启用功能、“IP/MAC 地址绑定的默认策略（允许或禁止）”，当该网口接收数据包时，将根据数据包中的源 IP 地址与源 MAC 地址，检查管理员设置好的 IP/MAC 地址绑定表。如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（允许或禁止）执行。

安全策略>>地址绑定

网口	启用IP/MAC绑定	默认策略
Fe1	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
Fe2	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
Fe3	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
Fe4	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
Fe5	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
Fe6	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
Fe7	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
Fe8	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
ge1	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
ge2	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
ge3	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）

主动探测IP/MAC对

按网口探测: Fe1 Fe2 Fe3 Fe4 Fe5 Fe6 Fe7 Fe8 ge1 ge2 ge3
 按 IP 探测:

已绑定IP/MAC对

IP地址	MAC地址	网口	检查双向绑定
无记录			
<input type="checkbox"/> 全选 <input type="button" value="添加"/> <input type="button" value="编辑"/> <input type="button" value="删除"/>			

◀ 首页
◀ 上一页
▶ 下一页
▶ 尾页
第1页/1页
跳转到

页

每页

行

本界面提供的功能：

1. 启用网络接口的 IP/MAC 绑定功能。

1. 探测 IP/MAC 地址对。其中，探测方式有两种：（1）按网口探测；（2）按 IP 探测。探测内容为当前流经安全网关的数据包的 IP 与 MAC 地址（不包括组播地址和安全网关地址）。

2. 绑定 IP/MAC 地址对。其中，绑定方式有两种：（1）探测 IP/MAC 地址对后选择并绑定；（2）手工输入 IP 与 MAC 对。

启用网络接口的 IP/MAC 绑定

网口	启用IP/MAC绑定	默认策略
fe1	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
fe2	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
fe3	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
fe4	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
fe5	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
fe6	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
fe7	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
fe8	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
ge1	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
ge2	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）
ge3	<input type="checkbox"/>	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止（没有绑定的IP/MAC所对应的策略）

确定

域 名	说 明
网口	显示安全网关的所有网络接口：FE1-FE8、GE1—GE3
启用 IP/MAC 绑定	启用该网口的 IP/MAC 绑定功能
默认策略	允许：设置 IP/MAC 绑定默认策略为“允许”。 禁止：设置 IP/MAC 绑定默认策略为“禁止”。

探测 IP/MAC 地址对


主动探测 IP/MAC 对

按网口探测:
 fe1
 fe2
 fe3
 fe4
 fe5
 fe6
 fe7
 fe8
 ge1
 ge2
 ge3

按 IP 探测:

域 名	说 明
按网口探测	<p>IP/MAC 地址探测方式</p> <p>显示当前已激活的网口列表（FE1—FE8、GE1—GE3），可以多选</p> <p>按网口探测 IP/MAC 地址对的操作步骤：</p> <ol style="list-style-type: none"> 1. 点击“安全策略>>地址绑定”菜单，弹出“安全策略>>地址绑定”界面。 2. 选择“按网口探测”，可以指定要做 IP/MAC 探测的网口（可以多选）。 3. 点击“探测”，将对指定网口进行 IP/MAC 地址对的探测。 4. 当网口前的选择消失后，点击“探测到的 IP/MAC 对”。 5. 弹出“探测到的 IP/MAC 地址对”界面，显示在指定网口当前探测到的 IP、MAC、网口，管理员可以根据探测到的 IP/MAC 地址对，完成绑定功能。 <p>参见：探测到的 IP/MAC 对的界面操作说明。</p>
按 IP 探测	<p>IP/MAC 地址探测方式，输入 IP 地址或网段</p> <p>按 IP 探测 IP/MAC 地址对的操作步骤：</p>

	<ol style="list-style-type: none"> 1. 点击“安全策略>>地址绑定”菜单，弹出“安全策略>>地址绑定”界面 2. 选择“按 IP 探测”，在输入框中输入 IP 地址或网段。 3. 点击“探测”，将对指定 IP 地址或网段进行 IP/MAC 地址对的探测。 4. 当“按 IP 探测”前的选择消失后，点击“探测到 IP/MAC 对”。 5. 弹出“探测到的 IP/MAC 地址对”界面，显示在指定网口当前探测到的 IP、MAC、网口，管理员可以根据探测到的 IP/MAC 地址对，完成绑定功能。 <p>参见 探测到的 IP/MAC 对的界面操作说明</p>
<p>操作</p>	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; padding: 2px 10px; background-color: #e0e0e0;">探测</div> 、 <div style="border: 1px solid black; padding: 2px 10px; background-color: #e0e0e0;">探测到的IP/MAC对</div> </div> <p>探测：对指定网口进行 IP/MAC 地址对的探测。探测完成时，指定网口前的选择号消失，管理员可以点击“探测到的 IP/MAC 对”进行查看。</p> <p>探测到的 IP/MAC 对：显示在指定网口当前探测到的 IP、MAC、网口的列表中。</p>

在“安全策略>>IP/MAC 地址绑定”界面中，点击 ，将弹出以下界面：



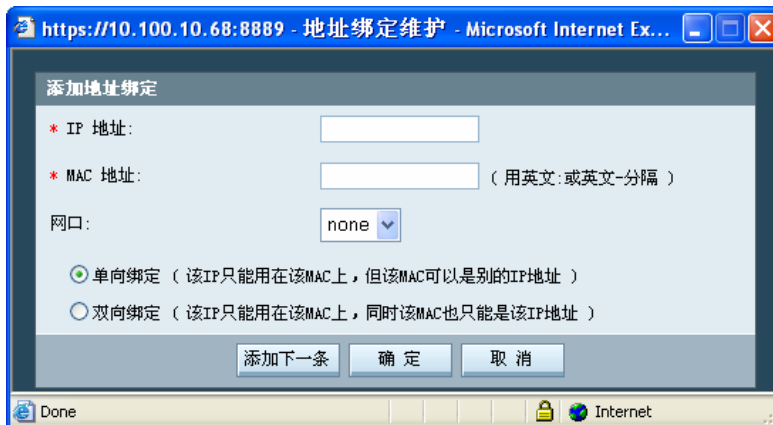
域 名	说 明
IP/MAC 对	输入要查找的 IP/MAC 对
查找	点击后，在该界面列表项中查找指定的地址对
选中	选择当前列表中的一项 IP/MAC 地址对
全选	选择当前列表中的全部 IP/MAC 地址对
IP 地址	探测到的 IP 地址，不能是组播地址
MAC 地址	探测到的 MAC 地址，不能是组播地址
网口	接收前述 IP/MAC 地址对的网口

检查双向绑定	当用户选择“检查双向绑定”时，安全网关会判断该 IP 只能用在该 MAC 上，同时该 MAC 也只能是该 IP 地址的数据包，如果匹配失败，则按照默认策略（允许或禁止）执行。
操作	绑定、删除、取消 ◇ 删除：从当前列表中删除选中的 IP/MAC 地址对 ◇ 绑定：将选中列表项中的 IP/MAC/网口进行绑定，绑定成功后的 IP/MAC 对将显示在已绑定 IP/MAC 对的列表中 ◇ 取消：取消本次操作

已绑定 IP/MAC 地址对

已绑定IP/MAC对			
IP地址	MAC地址	网口	检查双向绑定
<input type="checkbox"/> 10.100.10.57	00:CO:9F:EB:36:F1	fe1	<input checked="" type="checkbox"/>
<input type="checkbox"/> 全选 <input type="button" value="添加"/> <input type="button" value="编辑"/> <input type="button" value="删除"/>			

在“安全策略>>IP/MAC 地址绑定”界面中，点击 ，将弹出以下界面：



添加地址绑定

* IP 地址:

* MAC 地址: (用英文:或英文-分隔)

网口:

单向绑定 (该IP只能用在该MAC上, 但该MAC可以是别的IP地址)

双向绑定 (该IP只能用在该MAC上, 同时该MAC也只能是该IP地址)

域 名	说 明
IP 地址	要绑定的 IP 地址
MAC 地址	要绑定的 MAC 地址
网口	<p>可选择内容包括：none，安全网关所有已激活的网口。</p> <p>选择某网口，如果该网口设置了地址对绑定检查功能，当该 IP/MAC 地址对被此网口接收时，则进行地址对绑定检查。</p> <p>选择 none 时，则说明所有配置了绑定功能的网口在接收数据包时都做地址对绑定的检查。</p> <p>默认值为 none。</p>
单向绑定	<p>当用户选择“单向绑定”时，将检查数据包中的 IP 和 MAC 是否与安全网关系统中绑定的 IP 和 MAC 完全一致，必须一一对应；该 IP 只能用在该 MAC 上，但该 MAC 可以是别的 IP 地址，如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（允许或禁止）执行。</p>
双向绑定	<p>当用户选择“双向绑定”时，将检查数据包中的 IP 和 MAC 是否与安全网关系统中绑定的 IP 和 MAC 完全一致，必须一一对应；该 IP 只能用在该 MAC 上，同时该 MAC 也只能是该 IP 地址，如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（允许或禁止）执行。</p>
操作	添加下一条、确定、取消

	<ul style="list-style-type: none">◇ 添加下一条：添加本条规则成功后窗口仍旧打开，可以继续添加下一条规则◇ 确定：添加本条规则成功后关闭本窗口◇ 取消：取消本次操作
--	---

9.3. 安全策略>>IDS 联动

支持 IDS 产品联动，包括国内主流 IDS 产品。

当 IDS 联动产品发现入侵攻击行为时，会通知安全网关。如果安全网关相应网口启用了 IDS 自动阻断功能，则安全网关会按 IDS 产品通知的阻断方式、阻断时间和入侵主机的相关信息，对入侵主机进行阻断。

安全网关阻断方式包括：

- 对“源 IP 地址”阻断
- 对“源 IP 地址、目的 IP 地址、目的端口、协议”阻断、
- 对“源 IP 地址、目的 IP 地址、协议、方向（单向、双向、反向）”阻断

安全网关阻断协议包括：TCP / UDP / ICMP 和所有协议（any）。

安全策略>>IDS 联动

选择启用IDS阻断的网口

fe1
 fe2
 fe3
 fe4
 fe5
 fe6
 fe7
 fe8
 ge1
 ge2
 ge3












启用	产品名称	认证	IDS端IP地址 (多个用英文逗号分隔)	安全网关端服务端口
<input type="checkbox"/>	通用安全协议 (SUIP)入侵检测系统	导入密钥文件	<input type="text"/>	TCP <input type="text" value="5000"/> (默认: 5000)
<input type="checkbox"/>	“天闻” 入侵检测系统		<input type="text"/>	UDP <input type="text" value="2000"/> (默认: 2000)
<input type="checkbox"/>	“天眼” 入侵检测系统	导入证书	<input type="text"/>	TCP <input type="text" value="4000"/> (默认: 4000)
<input type="checkbox"/>	“SafeMate” 入侵检测系统	导入密钥文件	<input type="text"/>	UDP <input type="text" value="2001"/> (默认: 2001)

忽略对以下IP地址的自动阻断 (多个用英文逗号分隔)







域 名	说 明
选择启用 IDS 阻断的网口	显示了安全网关的 4 个网口，可以单击网口前面的复选框来启用该网络接口的 IDS 阻断。
启用与“通用安全协议(SUIP)入侵检测系统”联动	启用“通用安全协议(SUIP)入侵检测系统”后，选择正确的密钥文件导入，指定产品的 IP 地址、安全网关端的服务端口（默认 5000/UDP），安全网关可以与之联动。

启用与“天阆入侵检测系统”联动	启用“天阆入侵检测系统”后，指定产品的 IP 地址、安全网关端的服务端口（默认 2000/UDP），安全网关可以与之联动。
启用与“天眼入侵检测系统”联动	启用“天眼入侵检测系统”后，选择正确的证书导入，指定产品的 IP 地址、安全网关端的服务端口（默认 4000/TCP），安全网关可以与之联动。
启用与“saFEmate 入侵检测系统”联动	启用“saFEmate 入侵检测系统”后，选择正确的密钥文件导入，指定产品的 IP 地址、安全网关端的服务端口（默认 2001/UDP），安全网关可以与之联动。
忽略指定 IP 地址的自动阻断	当管理员不希望一些特别 IP 被安全网关阻断时，可以在“忽略以下 IP 地址的自动阻断”列表中加入这些 IP
清除已经阻断的 IP 地址	可以立即清除所有自动阻断。


9.4. 安全策略>>抗攻击

安全策略>>抗攻击										
接口名称	启用	SYN Flood	ICMP Flood	Ping of Death	UDP Flood	PING SWEEP	TCP端口扫描	UDP端口扫描	WinNuke	操作
fe1	✘	✘	✘	✘	✘	✘	✘	✘	✘	
fe2	✘	✘	✘	✘	✘	✘	✘	✘	✘	
fe3	✘	✘	✘	✘	✘	✘	✘	✘	✘	
fe4	✘	✘	✘	✘	✘	✘	✘	✘	✘	
fe5	✘	✘	✘	✘	✘	✘	✘	✘	✘	
fe6	✘	✘	✘	✘	✘	✘	✘	✘	✘	
fe7	✘	✘	✘	✘	✘	✘	✘	✘	✘	
fe8	✘	✘	✘	✘	✘	✘	✘	✘	✘	
ge1	✘	✘	✘	✘	✘	✘	✘	✘	✘	
ge2	✘	✘	✘	✘	✘	✘	✘	✘	✘	
ge3	✘	✘	✘	✘	✘	✘	✘	✘	✘	

抗攻击菜单说明：

域 名	说 明
接口名称	安全网关的通用网络接口：Fe1，Fe2，Fe3，Fe4，Fe5，Fe6，Fe7，Fe8，Ge1，Ge2，Ge3。
启用	 表示该网络接口启用抗攻击功能。  表示该网络接口没有启用抗攻击功能。
SYN Flood	 表示该网络接口启用“抗 SYN Flood 攻击”。  表示该网络接口不启用“抗 SYN Flood 攻击”。
ICMP Flood	 表示该网络接口启用“抗 ICMP Flood 攻击”。  表示该网络接口禁止“抗 ICMP Flood 攻击”。

Ping of Death	 表示该网络接口启用“抗 Ping of Death 攻击”。  表示该网络接口禁止“抗 Ping of Death 攻击”。
UDP Flood	 表示该网络接口启用“抗 UDP Flood 攻击”。  表示该网络接口禁止“抗 UDP Flood 攻击”。
PING SWEEP	 表示该网络接口启用“抗 PING SWEEP 攻击”。  表示该网络接口禁止“抗 PING SWEEP 攻击”。
TCP 端口扫描	 表示该网络接口启用“抗 TCP 端口扫描攻击”。  表示该网络接口禁止“抗 TCP 端口扫描攻击”。
UDP 端口扫描	 表示该网络接口启用“抗 UDP 端口扫描攻击”。  表示该网络接口禁止“抗 UDP 端口扫描攻击”。
WinNuke	 表示该网络接口启用“抗 WinNuke 端口扫描攻击”。  表示该网络接口禁止“抗 WinNuke 端口扫描攻击”。
操作	可以编辑  相关的抗攻击设置。

在抗攻击界面上，点击 ，可以针对该网口接收的数据包进行抗攻击处理。如下图所示：



各种抗攻击原理说明:

域 名	说 明
抗 SYN Flood 攻击	<p>攻击原理: TCP 连接是通过三次握手完成的。当网络中充满了发出无法完成的连接请求的 SYN 封包时,造成网络无法再处理合法的连接请求,从而导致拒绝服务(DoS)时,就发生了 SYN 泛滥攻击。攻击者通过不完全的握手过程消耗服务器的半开连接数目达</p>

	<p>到拒绝服务的攻击目的。攻击者向服务器发送 SYN 包，其中源 IP 地址已被改为伪造的不可达的 IP 地址。服务器向伪造的 IP 地址发出回应，并等待连接已建立的确认信息。但由于该 IP 地址是伪造的，服务器无法等到确认信息，只有保持半开连接状态直至超时。由于服务器允许的半开连接数目有限，如果攻击者发送大量这样的连接请求，服务器的半开连接资源很快就会消耗完毕，无法再接受来自正常用户的 TCP 连接请求。</p> <p>处理方法：管理员打开某网口的“抗 SYN Flood 攻击”检查，并设置 SYN 包速率阈值后，如果该网口接收的 TCP 连接超过预定阈值，就启用 SYN Proxy，安全网关将阻止 SYN 包直到已通过的 SYN 包的频率降到预定的域值以内。</p> <p>默认值为每秒 200 个数据包。</p>
抗 ICMP Flood 攻击	<p>攻击原理：当 ICMP ping 产生的大量回应请求超出了系统的最大限度，以至于系统耗费所有资源来进行响应直至再也无法处理有效的网络信息流时，就发生了 ICMP 泛滥。</p> <p>处理方法：管理员打开某网口的“抗 ICMP Flood 攻击”检查，并设置 ICMP 包速率阈值后，该网口将过滤发往广播地址的 ICMP 包，同时对发往单个 IP 地址的 ICMP 包进行频率统计，一旦达到预定的域值就会调用 ICMP 泛滥攻击保护功能，安全网关将阻止 ICMP 包直到已通过的 ICMP 包的频率降到预定的域值以内。</p>

	<p>默认值为每秒 1000 个数据包。</p>
<p>抗 Ping of Death 攻击</p>	<p>攻击原理：TCP/IP 规范要求用于数据包传输的封包必须具有特定的大小。许多 ping 允许用户根据需要指定更大的封包大小。当攻击者发送超长的 ICMP 包时会引发一系列负面的系统反应，早期的操作系统可能因为缓冲区溢出而宕机，如拒绝服务(DoS)、系统崩溃、死机以及重新启动。</p> <p>处理方法：管理员打开某网口的“抗 Ping of Death 攻击”检查，并设置 ICMP 包长阈值后，该网口将过滤长度超过预定域值的 ICMP 包。</p> <p>默认值为 800 字节</p>
<p>抗 UDP Flood 攻击</p>	<p>攻击原理：与 ICMP 泛滥相似。攻击者向同 IP 地址发送大量的 UDP 包使得该 IP 地址无法响应其它 UDP 请求，就发生了 UDP 泛滥。</p> <p>处理方法：管理员打开某网口的“抗 UDP Flood 攻击”检查，并设置 UDP 包速率阈值后，如果该网口对接收的每个 IP 地址的 UDP 包进行频率统计，一旦超过此临界值就会调用 UDP 泛滥攻击保护功能，如果从一个或多个源向单个目标发送的 UDP 封包数超过了此临界值，安全网关将立即忽略其它到该目标的 UDP 包，直到通过的 UDP 包频率降到预定的域值以内。</p> <p>默认值为每秒 1000 个数据包。</p>
<p>抗 PING</p>	<p>攻击原理：攻击者向某个网段的多个 IP 地址发送 ICMP 包（尤以</p>

SWEEP 攻击	<p>PING 包为主), 探测 IP 地址是否存在, 如果某个 IP 地址发出响应则可能被选定为攻击目标。</p> <p>处理方法: 管理员打开某网口的“抗 PING SWEEP 攻击”检查并设置 PING SWEEP 阈值后, 如果发现网口接收的某个 IP 地址在指定阈值时间内向 10 个不同 IP 地址发送 ICMP 包就会调用 PING SWEEP 保护功能, 阻断来自该 IP 地址的 ICMP 包 5 秒钟, 不管其目的 IP 是多少。在阻断期内如果再次发现 PING SWEEP 攻击则延长阻断时间至攻击发现时刻后的 5 秒钟。</p> <p>默认值为每 10ms 发送到 10 个 IP 被判为攻击。</p>
抗 TCP 端口扫描	<p>攻击原理: 攻击者向同一 IP 的多个 TCP 端口发起连接, 探测目的主机开启的服务, 为后续攻击做准备。</p> <p>处理方法: 管理员打开某网口的“抗 TCP 端口扫描”检查, 并设置 TCP 端口扫描阈值后, 如果发现网口接收的某个 IP 地址在指定阈值时间内向同一 IP 的 10 个不同端口发送 TCP 包, 就会调用 TCP 端口扫描保护功能, 阻断来自该 IP 地址的 TCP 包 5 秒钟, 不管其目的 IP 和目的端口是多少。在阻断期内如果再次发现 TCP 端口扫描攻击则延长阻断时间至攻击发现时刻后的 5 秒钟。</p> <p>默认值为每 10ms 发送到同一 IP 的 10 个 TCP 端口被判为攻击。</p>
抗 UDP 端口扫描	<p>攻击原理: 攻击者向同一 IP 的多个 UDP 端口发起连接, 探测目的主机开启的服务, 为后续攻击做准备。</p>

	<p>处理方法：管理员打开某网口的“抗 UDP 端口扫描”检查，并设置 UDP 端口扫描阈值后，如果发现网口接收的某个 IP 地址在指定阈值时间内向同一 IP 的 10 个不同端口发送 UDP 包就会调用 UDP 端口扫描保护功能，阻断来自该 IP 地址的 UDP 包 5 秒钟，不管其目的 IP 和目的端口是多少。在阻断期内如果再次发现 UDP 端口扫描攻击则延长阻断时间至攻击发现时刻后的 5 秒钟。</p> <p>默认值为每 10ms 发送到同一 IP 的 10 个 UDP 端口被判为攻击。</p>
<p>抗松散源路由攻击</p>	<p>攻击原理：IP 包头信息有一个选项，其中包含的路由信息可指定与包头源路由不同的源路由。“松散源路由选项”可允许攻击者以假的 IP 地址进入网络，并将数据送回其真正的地址。</p> <p>处理方法：管理员打开某网口的“抗松散源路由攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
<p>抗严格源路由攻击</p>	<p>攻击原理：IP 包头信息有一个选项，其中包含的路由信息可指定与包头源路由不同的源路由。“严格源路由选项”可允许攻击者以假的 IP 地址进入网络，并将数据送回其真正的地址。</p> <p>处理方法：管理员打开某网口的“抗严格源路由攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
<p>抗 WinNuke 攻击</p>	<p>攻击原理：WinNuke是一种常见的应用程序，其唯一目的就是使互联网上任何运行 Windows 的计算机崩溃。这种专门针对 Windows3.1/95/NT 的攻击曾经猖獗一时，受攻击的主机在片刻间</p>

	<p>出现蓝屏现象（系统崩溃）。WinNuke通过已建立的连接向主机发送带外(OOB)数据，通常发送到NetBIOS端口（TCP139端口），攻击者只要先跟目标主机的139端口建立连接，继而发送一个带URG标志的带外数据报文，引起NetBIOS碎片重叠，目标系统即告崩溃。重新启动后，会显示下列信息，指示攻击已经发生：</p> <p>An exception OE has occurred at 0028:[address] in VxD MSTCP(01)+000041AE. This was called from 0028:[address] in VxD NDIS(01)+00008660. It may be possible to continue normally.（有可能继续正常运行。）</p> <p>Press any key to attempt to continue.（请按任意键尝试继续运行。）</p> <p>Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.（按CTRL+ALT+DEL 可尝试继续运行。将丢失所有应用程序中的未保存信息。）</p> <p>Press any key to continue.（按任意键继续。）</p> <p>原因是系统中某些端口的监听程序不能处理“意外”来临的带外数据，造成严重的非法操作。</p> <p>处理方法：管理员打开某网口的“抗 WinNuke 攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
抗 smurf 攻击	<p>攻击原理：攻击者伪装成被攻击主机向广播地址发送 ICMP 包（以 PING 包为主），这样被攻击主机就可能收到大量主机的回应，攻</p>

	<p>击者只需要发送少量攻击包，被攻击主机就会被淹没在 ICMP 回应包中，无法响应正常的网络请求。</p> <p>处理方法：管理员打开某网口的“抗 smurf 攻击”检查，对收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
<p>抗 TCP 无标记攻击</p>	<p>攻击原理：正常数据包中，至少包含 SYN、FIN、ACK、RST 四个标记中的一个，不同的 OS 对不包含这四个标记中任何一个标志的数据包有不同处理方法，攻击者可利用这种数据包判断被攻击主机的 OS 类型，为后续攻击做准备。</p> <p>处理方法：检查接收到的数据包，禁止符合此攻击特征的包通过。</p>
<p>抗圣诞树攻击</p>	<p>攻击原理：正常数据包中，不会同时包含 SYN、FIN、ACK、RST 四个标记，不同的 OS 对包含全部四个标志的数据包有不同处理方法，攻击者可利用这种数据包判断被攻击主机的 OS 类型，为后续攻击做准备。</p> <p>处理方法：检查接收到的数据包，禁止符合此攻击特征的包通过。</p>
<p>抗 SYN&FIN 位设置攻击</p>	<p>攻击原理：正常数据包中，不会同时设置 TCP Flags 中的 SYN 和 FIN 标志，因为 SYN 标志用于发起 TCP 连接，而 FIN 标志用于结束 TCP 连接。不同的 OS 对同时包含 SYN 和 FIN 标志的数据包有不同处理方法，攻击者可利用这种数据包判断被攻击主机的 OS 类型，为后续攻击做准备。</p> <p>处理方法：检查接收到的数据包，禁止符合此攻击特征的包通过。</p>

抗无确认 FIN 攻击	<p>攻击原理：正常数据包中，包含 FIN 标志的 TCP 数据包同时包含 ACK 标志。不同的 OS 对包含 FIN 标志但不包含 ACK 标志的数据包有不同处理方法，攻击者可利用这种数据包判断被攻击主机的 OS 类型，为后续攻击做准备。</p> <p>处理方法：检查接收到的数据包，禁止符合此攻击特征的包通过。</p>
抗 IP 安全选项攻击	<p>攻击原理：IP 包头信息有一个选项，目前已经废除，因此数据包中出现这个选项则很可能是攻击行为。</p> <p>处理方法：管理员打开某网口的“抗 IP 安全选项攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
抗 IP 记录路由攻击	<p>攻击原理：IP 包头信息有一个选项，攻击者可利用这个选项收集被攻击主机周围的网络拓扑等信息，为后续攻击做准备。</p> <p>处理方法：管理员打开某网口的“抗 IP 记录路由攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
抗 IP 流攻击	<p>攻击原理：IP 包头信息有一个选项，目前已经废除，因此数据包中出现这个选项则很可能是攻击行为。</p> <p>处理方法：管理员打开某网口的“抗 IP 流攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
抗 IP 时间戳攻击	<p>攻击原理：IP 包头信息有一个选项，攻击者可利用这个选项收集被攻击主机周围的网络拓扑等信息，为后续攻击做准备。</p> <p>处理方法：管理员打开某网口的“抗 IP 时间戳攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>

	<p>收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
抗 Land 攻击	<p>攻击原理：“陆地”攻击将 SYN 攻击和 IP 欺骗结合在了一起，当攻击者发送含有受害方 IP 地址的欺骗性 SYN 包，将其作为目的和源 IP 地址时，就发生了“陆地”攻击。接收系统通过向自己发送 SYN-ACK 封包来进行响应，同时创建一个空的连接，该连接将会一直保持到达到空闲超时值为止。向系统堆积过多的这种空连接会耗尽系统资源，导致 DoS。攻击者发送特殊的 SYN 包，其中源 IP 地址、源端口和目的 IP 地址、目的端口指向同一主机，早期的操作系统收到这样的 SYN 包时可能会宕机。</p> <p>处理方法：管理员打开某网口的“抗 Land 攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。</p>
抗 tear drop 攻击	<p>攻击原理：数据包通过不同的网络时，有时必须根据网络的最大传输单位(MTU)将数据包分成更小的部分（片断）。攻击者可能会利用 IP 栈具体实现的数据包重新组合代码中的漏洞，通过 IP 碎片进行攻击。teardrop 是利用早期某些操作系统中 TCP/IP 协议栈对 IP 分片包进行重组时的漏洞进行的攻击，受影响的系统包括 Windows 3.1/95/NT 以及 Linux2.1.63 之前的版本，其结果是直接导致系统崩溃，Windows 系统则表现为典型的蓝屏症状。这一问题存在的直接原因在于：当目标系统收到这些封包时，一些操作系统的 TCP/IP 协议栈的实现中，对接收到的 IP 分片进行重组时，</p>

没有考虑到一种特殊的分片重叠，导致系统非法操作。

处理方法：管理员打开某网口的“抗 tear drop 攻击”检查，对接收到的数据包进行检查，禁止符合此攻击特征的包通过。

9.5. 安全策略>>P2P 限制

P2P 技术是一种用于不同 PC 用户之间、不经过中继设备直接交换数据或服务的技术。它打破了传统的 Client/Server 模式，在对等网络中，每个节点的地位都是相同的，具备客户端和服务端双重特性，可以同时作为服务使用者和服务提供者。由于 P2P 技术的飞速发展，互联网的存储模式将由目前的“内容位于中心”模式转变为“内容分散存储”模式，改变了 Internet 现在的以大网站为中心的流量状态。现在网上常用的 P2P 软件主要有 BT、eDonkey、eMule 等。P2P 技术主要带来了如下一些变化：

Internet 上流量模型的变化，现在 Internet 上 70% 的流量都是 P2P 的流量，而传统的 HTTP 流量已经不是 Internet 上的主要流量。

个人用户的流量模型的变化。以前个人用户的下行流量（从 Internet 到个人用户）远远大于上行流量。而由于 P2P 技术在下载的同时，也需要上传。导致个人用户的下行流量和上行流量都很大。P2P 流量造成网络的极度拥塞。

SecGate 3600-G10 安全网关对 P2P 软件采用深度检测的方法，可以精确的识别 P2P 流量，以达到对 P2P 流量进行控制的目的。

在“安全策略”界面中，点击 ，将弹出以下界面：

安全策略 >> P2P 限制

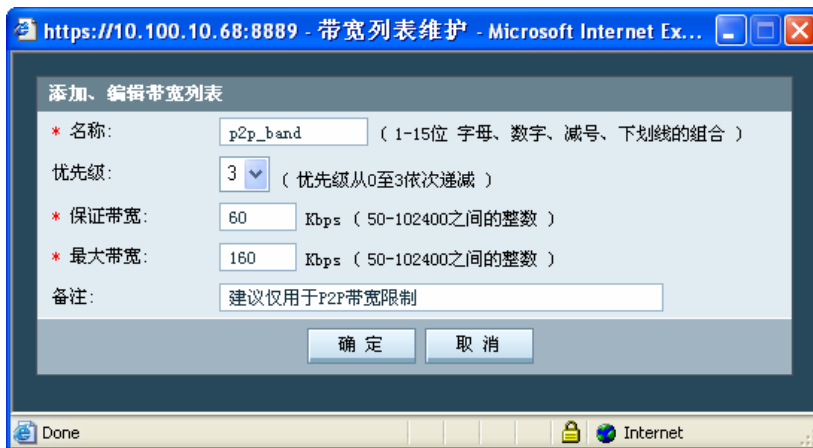
P2P 协议	动作
apple	禁止使用
ares	允许使用不做任何限制
bt	允许使用且进行流量控制
dc	允许使用不做任何限制
edonkey	禁止使用
gnu	禁止使用
kazaa	禁止使用
soul	禁止使用
winx	禁止使用
流量控制:	p2p_band (注: 此处为以上协议加起来的带宽和)

确定

P2P 协议	动作
apple	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制
ares	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制
bt	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制
dc	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制
edonkey	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制
gnu	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用

	三种动作控制
Kazaa	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制
Soul	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制
Winmx	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制
流量控制	可以针对该 P2P 协议做允许使用不做任何限制、禁止使用、允许使用三种动作控制

在“对象定义>>带宽列表”中，针对 P2P 做了默认的带宽控制规则。



所有的 P2P 协议共享一个带宽列表

9.6. 安全策略>>连接限制

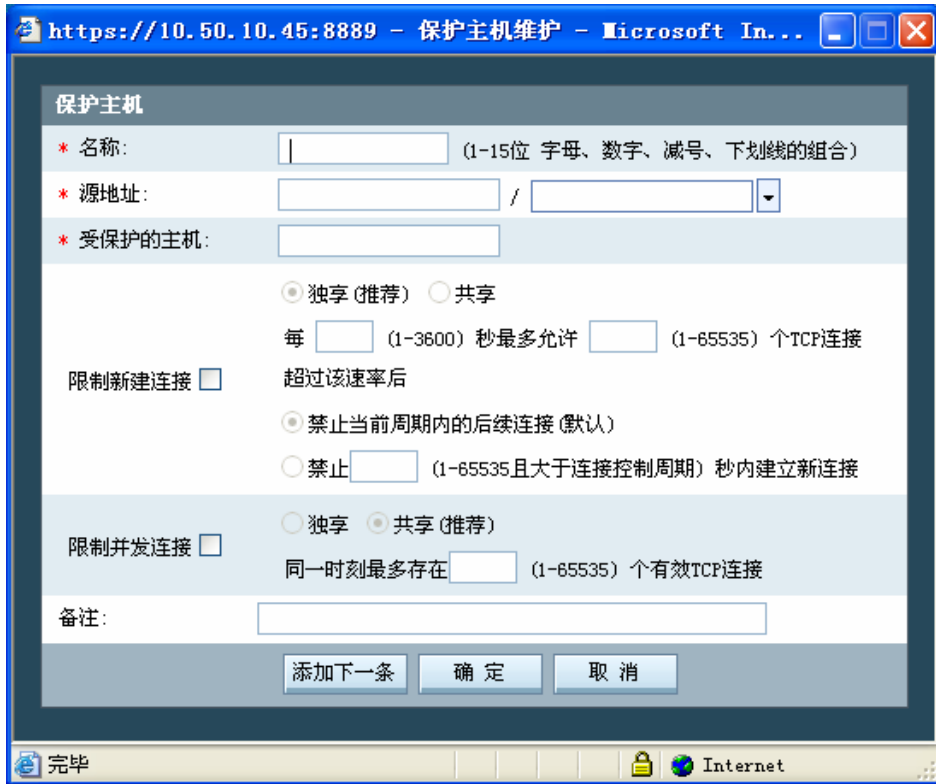
连接限制是为了保护服务器，限制对服务器过于频繁的访问。在规定的时间内，如果某台主机访问服务器超过了所限制的次数，则会对该主机实行阻断，在阻断时间段内，拒绝其对服务器的所有访问。在“对象定义>>连接限制”中，提供了四种连接限制：保护主机、保护服务、限制主机、限制服务。

9.6.1. 保护主机

保护主机是指对访问的目的地址服务器进行保护，限制对此地址服务器的访问过于频繁。

序号	名称	源地址	受保护主机	限制新建	限制开发	备注	操作
1	protest1	10.50.10.23/255.255.255.255	192.168.1.1	✓	✓		 
2	www	10.50.10.23/255.255.255.255	10.50.10.22	✓	✓		 

在“安全策略>>连接限制>>保护主机”界面中，点击 ，将弹出以下界面：



保护主机

* 名称: (1-15位 字母、数字、减号、下划线的组合)

* 源地址: /

* 受保护的主机:

独享 (推荐) 共享

每 (1-3600) 秒最多允许 (1-65535) 个TCP连接

限制新建连接 超过该速率后

禁止当前周期内的后续连接 (默认)

禁止 (1-65535且大于连接控制周期) 秒内建立新连接

限制并发连接 独享 共享 (推荐)

同一时刻最多存在 (1-65535) 个有效TCP连接

备注:

添加下一条 确定 取消

值 域	说 明
源地址	客户端的 IP 地址或网段
受保护的主机	被保护的服务器地址
限制新建连接	限制客户端向服务器新发起的连接数 独享：控制每个客户端向服务器发起的连接数，如果该客户端发起的连接数超过规定数目，则安全网关做相应的处理。 共享：控制所有客户端向服务器发起的连接数的和，如果超过规定数目则安全网关做相应处理

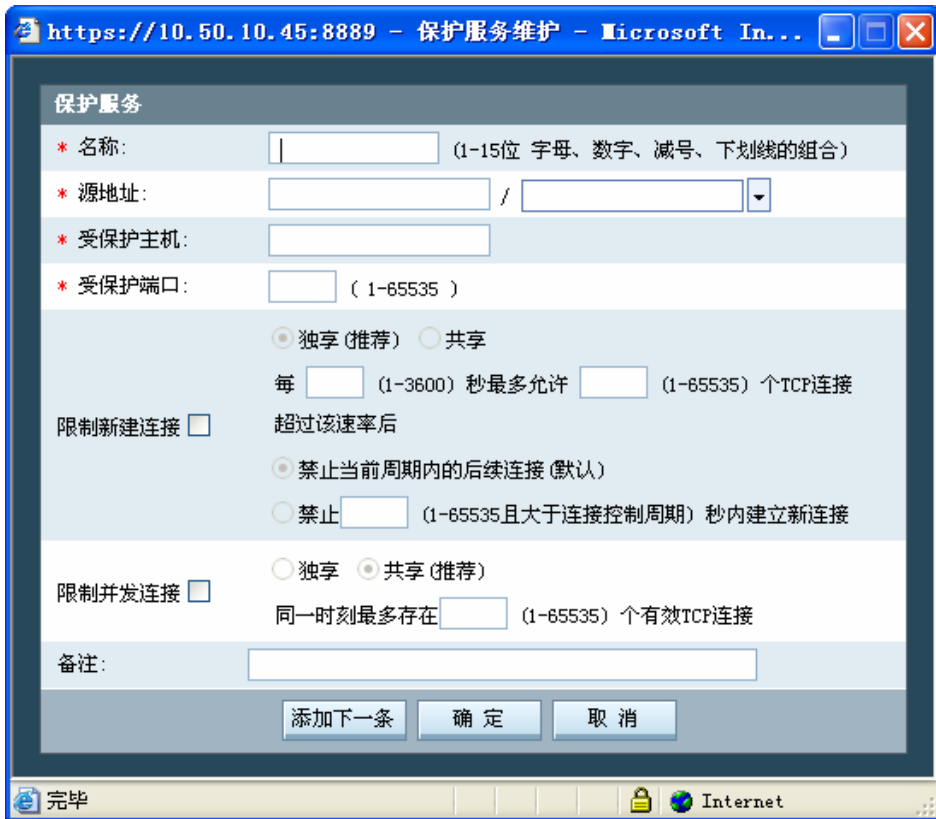
	<p>定义一个连接限制，限制任何主机在规定的时间内对服务器的访问不能超过规定的次数。</p>
<p>超过该速率后</p>	<p>“禁止当前周期的后续连接”指客户端在每个时间周期内都可以访问服务器，但是每个周期内的连接数不能超过规定连接数，连接次数不计入下一个周期。</p> <p>“禁止建立新连接”指客户端向服务器发起的连接数一旦超过规定数目，就中断一段时间，无论是否已经进入下一个时间周期。</p>
<p>限制并发连接</p>	<p>限制客户端与服务器已经建立并且未中断的连接。</p> <p>独享：限制客户端与服务器已经建立并且未中断的连接的数目，不影响其它客户端与服务器建立连接。</p> <p>共享：限制所有客户端与服务器已经建立并且未中断的连接的数目之和。</p> <p>“同一时间存在的有效的 TCP 连接数”指客户机与服务器已经建立并且未中断的连接数目，如果超过这个数目，安全网关将执行相关的处理</p>

9.6.2. 保护服务

保护服务是指被访问服务器提供的某类服务进行保护，限制对此服务器的这类服务进行过于频繁的访问。

序号	名称	源地址	受保护主机/端口	限制新建	限制并发	备注	操作
1	protect1	192.168.1.0/255.255.255.0	10.50.10.1/80	✓	✓		 

在“安全策略>>连接限制>>保护服务”界面中，点击 ，将弹出以下界面：



保护服务

* 名称: (1-15位 字母、数字、减号、下划线的组合)

* 源地址: /

* 受保护主机:

* 受保护端口: (1-65535)

独享 (推荐) 共享

每 (1-3600) 秒最多允许 (1-65535) 个TCP连接
超过该速率后

限制新建连接

禁止当前周期内的后续连接 (默认)

禁止 (1-65535且大于连接控制周期) 秒内建立新连接

限制并发连接

独享 共享 (推荐)

同一时刻最多存在 (1-65535) 个有效TCP连接

备注:

Internet

值 域	说 明
源地址	客户端的 IP 地址或网段

受保护的主机	被保护的服务器地址
受保护端口	被保护的服务器端口
限制新建连接	<p>限制客户端向服务器新发起的连接数</p> <p>独享：控制每个客户端向服务器发起的连接数，如果该客户端发起的连接数超过规定数目，则安全网关做相应的处理。</p> <p>共享：控制所有客户端向服务器发起的连接数的和，如果超过规定数目则安全网关做相应处理</p> <p>定义一个连接限制，限制其它主机在规定的时间内对服务器的访问不能超过规定的次数。</p>
超过该速率后	<p>“禁止当前周期的后续连接”指客户端在每个时间周期内都可以访问服务器，但是每个周期内不能超过规定连接数，连接次数不计入下一个周期。</p> <p>“禁止建立新连接”指客户端向服务器发起的连接数一旦超过规定数目，就中断一段时间，无论是否已经进入下一个时间周期。</p>
限制并发连接	<p>限制客户端与服务器已经建立并且未中断的连接。</p> <p>独享：限制客户端与服务器已经建立并且未中断的连接的数目，不影响其它客户端与服务器建立连接。</p> <p>共享：限制所有客户端与服务器已经建立并且未中断的连接的数目之和。</p>

“同一时间存在的有效的 TCP 连接数”指客户机与服务器已经建立并且未中断的连接数目，如果超过这个数目，安全网关将执行相关的处理。

9.6.3. 限制主机

限制主机是指对发起访问的源地址的机器进行限制，限制此地址对服务器发起过于频繁的申请。

序号	名称	受限地址	限制新建	限制开发	备注	操作
1	aaa	1.1.1.1/255.255.255.255	✓	✗	jfjf	 
2	protext2	10.50.10.100/255.255.255.255	✓	✓		 

在“安全策略>>连接限制>>限制主机”界面中，点击 ，将弹出以下界面：



值 域	说 明
受限制的地址	被限制的客户端地址
限制新建连接	限制客户端向服务器新发起的连接数 独享：控制每个客户端向服务器发起的连接数，如果该客户端发起的连接数超过规定数目，则安全网关做相应处理。 共享：控制所有客户端向服务器发起的连接数的和，如果超过规定数目则安全网关做相应处理 定义一个连接限制，限制其它主机在规定的时段内对服务器

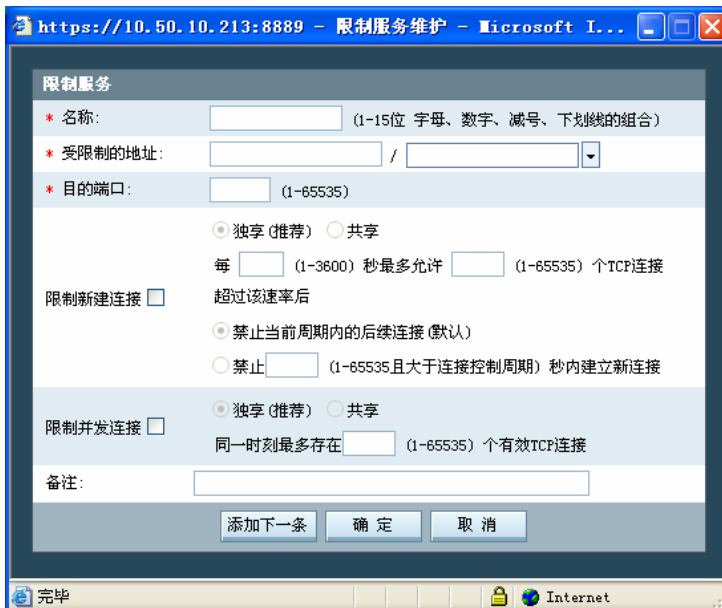
	<p>的访问不能超过规定的次数。</p>
<p>超过该速率后</p>	<p>“禁止当前周期的后续连接”指客户端在每个时间周期内都可以访问服务器，但是每个周期内不能超过规定连接数，连接次数不计入下一个周期。</p> <p>“禁止建立新连接”指客户端向服务器发起的连接数一旦超过规定数目，就中断指定的秒数，无论是否已经进入下一个时间周期。</p>
<p>限制并发连接</p>	<p>限制客户端与服务器已经建立并且未中断的连接。</p> <p>独享：限制客户端与服务器已经建立并且未中断的连接的数目，不影响其它客户端与服务器建立连接。</p> <p>共享：限制所有客户端与服务器已经建立并且未中断的连接的数目之和。</p> <p>“同一时间存在的有效的 TCP 连接数”指客户机与服务器已经建立并且未中断的连接数目，如果超过这个数目，安全网关将执行相关的处理</p>

9.6.4. 限制服务

限制服务是指对发起访问的源地址的机器访问某类服务进行限制，限制此地址对服务器的此类服务发起过于频繁的申请。

序号	名称	受限地址	目的端口	限制新建	限制并发	备注	操作
1	protect1	10.50.10.100/255.255.255.255	80	✓	✗		 

在“安全策略>>连接限制>>限制服务”界面中，点击 ，将弹出以下界面：



值 域	说 明
受限的地址	被限制的客户端地址
目的端口	客户端访问服务器的这个端口将被限制，可选的端口范围是 1 到 65535
限制新建连接	限制客户端向服务器新发起的连接数

	<p>独享：控制每个客户端向服务器发起的连接数，如果该客户端发起的连接数超过规定数目，则安全网关做相应处理。</p> <p>共享：控制所有客户端向服务器发起的连接数的和，如果超过规定数目则安全网关做相应处理</p> <p>定义一个连接限制，限制其它主机在规定的时间内对服务器的访问不能超过规定的次数。</p>
<p>超过该速率后</p>	<p>“禁止当前周期的后续连接”指客户端在每个时间周期内都可以访问服务器，但是每个周期内不能超过规定连接数，连接次数不计入下一个周期。</p> <p>“禁止建立新连接”指客户端向服务器发起的连接数一旦超过规定数目，就中断一段时间，无论是否已经进入下一个时间周期。</p>
<p>限制并发连接</p>	<p>限制客户端与服务器已经建立并且未中断的连接。</p> <p>独享：限制客户端与服务器已经建立并且未中断的连接的数目，不影响其它客户端与服务器建立连接。</p> <p>共享：限制所有客户端与服务器已经建立并且未中断的连接的数目之和。</p> <p>“同一时间存在的有效的 TCP 连接数”指客户机与服务器已经建立并且未中断的连接数目，如果超过这个数目，安全网关将执行相关的处理</p>

10. 高可用性

SecGate 3600 安全网关支持路由高可用性，能够实现主动-被动模式(双机热备)、主动-主动模式(负载均衡)、链路探测工作模式。在一台安全网关出现问题时，其它安全网关可以及时接管路由转发工作，向用户提供透明的切换，提高了网络服务质量。

- **主动-被动模式(双机热备):** 集群中所有节点的 IP 和 MAC 地址相同。一台安全网关为主节点，处于工作中，负责处理所有的网络流量以及整个集群的控管；其它安全网关节点为从节点，处于热备中，接收到网络数据包后，全部丢弃。一旦主节点发生故障，优先级次之的从节点升为主节点，接管原来主节点的工作，保证网络正常通信。切换时间小于 1 秒。主从安全网关的配置信息可以手工同步并生效。提供日志记录和报警邮件。
- **主动-主动模式(负载均衡):** 集群中所有节点的 IP 和 MAC 地址相同，协同工作且负载均衡。一台安全网关是主节点，处于工作中，负责处理部分网络流量以及整个集群的控管；其它安全网关节点为从节点，也处于工作中，和主节点一起分担部分网络流量。当两台安全网关都处于正常工作状态时，双方的状态信息同步，可以对网络流量、带宽等进行动态平衡，而且当网络负荷不断提高时，两台安全网关可同时发挥自身的最高能力以避免瓶颈的形成；当一台安全网关出现故障而停机，另一台可以立即接管其工作，而且切换对用户完全透明，无切换时间。负

载均衡中的安全网关，其状态信息自动同步，配置信息启动时自动同步，其它时间可以点“配置同步”及时同步生效。提供日志记录和报警邮件。负载均衡模式支持 2 到 4 台安全网关，可以满足对可靠性和性能要求非常高的用户。

- 链路探测：双机热备和负载均衡模式下，提供按 IP 地址和网口进行链路探测的功能。根据探测结果可以调整集群安全网关的失效状态，均衡负载。

10.1. 高可用性>>HA 基本参数

高可用性>>HA基本参数

HA网口地址

HA网口IP: (同一集群中的各节点的HA接口IP必须不相同,但属于同一网段)

掩码: ▾

HA基本参数

启用HA:

HA标识符: (1~255,同一集群中的各节点HA标识符必须相同)

工作模式: 双机热备 负载均衡 双链路冗余 (同一集群中的各节点工作模式必须相同)

本节点为: 号节点 (同一集群中,节点序号必须唯一)

网口属性: 单播 多播

同步网络会话状态表的网口: ▾

说明: 启用配置同步时,请您在安全策略中添加“允许另一台防火墙访问本防火墙secgate_ha_conf服务”的包过滤规则

HA 基本配置菜单说明：

域 名	说 明
HA 网口 IP	HA 口的 IP 地址。 HA 口可以用于 HA 功能，也可以用于连接日志服务器。

当使用安全网关集群功能时，要求各节点 HA 口的 IP 为同一网段的不同 IP 地址，并将多台安全网关的 HA 口连接，用于集群的心跳检测。

心跳协议在 UDP 6666 端口进行通讯，整个 SLBP 集群有一个主节点和多个从节点。

主节点周期性地(周期为 0.5 秒)广播自己的心跳信号给各从节点；从节点周期性地(周期为 0.5 秒)单播自己的心跳信号给主节点。

如果主节点在规定时间内(缺省为 2 秒钟)没有收到某一从节点的心跳信号，则认为该从节点已经离线，主节点会自动进行下列动作：

- ◇ **主从热备模式下：**主节点会继续负责处理所有的网络流量，删除 SLBP 集群节点表中该节点的信息，并调节其它各从节点的优先级，同时报警和记日志。
- ◇ **负载均衡模式下：**主节点会删除 SLBP 集群节点表中该节点的信息，调节自己的负载以及其它各从节点的优先级和负载，同时报警和记日志。

如果主节点离线了，优先级为 2 的从节点会在规定时间内(缺省为 2 秒钟)没有收到主节点的心跳信号，认为主节点已经离线，该节点会自动进行下列动作：

- ◇ **主从热备模式下：**该节点会自动升为主节点来控管整个 SLBP 集群，负责处理所有的网络流量，并删除 SLBP 集群的节点

	<p>状态表中原来主节点，调节其它各从节点的优先级，同时报警和记日志。</p> <p>✧ 负载均衡模式下：该节点会自动升为主节点来控管整个 SLBP 集群，并删除 SLBP 集群的节点状态表中原来主节点，并调节其它各从节点的优先级。重新分配 SLBP 集群中剩余节点的负载，同时报警和记日志。</p> <p>注意：配置或修改 HA 口 IP 地址，当未启用 HA 功能时，安全网关不需要重启；当启用 HA 功能时，安全网关需要重启。界面会有相关提示信息。</p>
掩码	HA 口的 IP 地址的掩码
启用 HA	是否启用 HA
HA 标识符	<p>SLBP 集群的 ID。范围:1 — 255</p> <p>同一集群中的各节点 HA 标识符必须相同。只有具有相同 HA 标识符的节点之间才可以互相进行心跳通讯，才可以属于一个 SLBP 集群。</p>
工作模式	<p>双机热备或负载均衡，同一集群中的各节点工作模式必须相同。</p> <p>双机热备：两台安全网关均加电，但只有主安全网关在工作状态，从安全网关在监听状态，当主安全网关宕机时，从安全网关将立即接替主安全网关工作。</p> <p>负载均衡：最多为 4 台安全网关同时工作，只有一台为主安全网</p>

	<p>关。负载按 HASH 算法在各节点上均衡。通过主安全网关监控集群中各节点工作。其中，用户认证信息、非 IP 协议数据包等只由主安全网关处理。</p> <p>双链路冗余模式：类似负载均衡模式，主要应用在已经具有负载均衡功能的路由器或交换机的网络环境中，或者应用在通过 STP，OSPF 或 EIGRP 等协议自动选择路径的网络环境中。集群中所有节点都处于主动工作中(只能工作在透明桥模式)，负责处理流经自身节点的网络数据流。一旦双链路中的任何一条链路的安全网关节点发生故障，另外一条链路的安全网关节点会接管失效链路的会话，保证网络正常通信。</p> <p>注意：由于具有负载均衡器，或者具有自动选路特征的网络环境能够确保任何一个数据帧只会流经一个安全网关节点，而不会形成回环。注意这种模式一定要保证网络不会形成数据帧的回环。</p>
节点	节点序号，同一集群中节点序号必须唯一。
网口属性	选择 fe1-fe8, ge1-ge3 各个网口的 mac 地址是单播地址还是多播地址。
同步网络会话状态表的网口	主与从安全网关间需要同步网络会话状态表，可以选择通过哪个数据通信网口进行。
<div style="border: 1px solid black; padding: 2px; display: inline-block;">查看HA状态</div>	点击“查看 HA 状态”按钮，进入“系统监控>>HA 状态”界面。

查看 HA 状态:

在“网络配置>>HA 基本参数”界面中, 点击按钮 [查看HA状态](#), 转到以下界面:

系统监控>>HA状态				
节点号	优先级	HA网口IP地址	配置同步状况	详细状态
3	1	1.2.3.4	已同步	详细
		同步所有节点的配置	刷新	

菜单说明:

域 名	说 明
节点号	集群中各安全网关做为节点的 ID 号。 同一个 SLBP 集群中该节点的唯一标识。同一个 SLBP 集群中的的各安全网关节点 ID 号必须唯一。
优先级	各节点的优先级。 同一个 SLBP 集群, 最早加入集群的安全网关节点(即最早启动完毕的安全网关节点)的优先级为 1, 该节点是主节点; 第二个加入集群的安全网关节点优先级为 2, 依次类推, 这些节点为从节点。负载均衡中, 当主安全网关宕机后, 优先级高的先接替其工作。 需要注意的是: 如果节点优先级为 0, 表示该节点处于失效状态((HA 路径监控工具监控到本节点和周边设备连接出现故障后, 会置本节点为失效), 不能处理任何网络业务数据, 只有当该节点的优先级大于 0, 即该节点又重新恢复有效状态, 才可以处理网络业务数据。
HA 网口 IP 地	各安全网关节点上的 HA 口的 IP 地址。

址	一个集群中各节点的 HA 口的 IP 地址应在一个网段中。
配置同步状况	各安全网关节点与主安全网关配置信息同步的情况。
详细状态	点击“详细”，则显示该 HA 节点当前的 IP、ID、优先级、配置同步状况、监控的网口状态、监控的周边设备状态。 参考“系统监控>>HA 状态” 系统监控>>HA状态 。



当安全网关集群中有节点离线时，主安全网关会发出报警邮件。前提是正确配置了报警邮箱和 DNS 服务器。

10.2. 高可用性>> HA 监控网口

HA 路径监控对于用户了解 SLBP 集群中的安全网关设备连接状况是很有用的工具，用它可以检查安全网关网络接口和其它设备接口之间的第 2 层和第 3 层网络连接是否有效。

网口监控属于第 2 层路径监控的功能，是检查安全网关设备的物理网口是否处于活动状态并连接到周边网络设备。如果安全网关管理员定义了一个需要 HA 监控的网口，而该网口的监控结果是 Link Down 状态，则该安全网关节点将进入失效状态。当监控网口的监控结果是 Link Up 状态，该安全网关节点会从失效状态重新转变为有效状态。根据探测结果可以调整集群安全网关的失效状态，以便均衡负载。

如果没有启用 HA 功能，则在本页面显示如下信息：



信息：未启用HA，故无法设置HA监控网口。

如果启用了 HA 功能，本页面显示如下信息：

系统监控>>HA监控网口

如果下列选中的网口连接失败，则置本防火墙为失效

ge1
 ge2
 ge3
 fe1
 fe2
 fe3
 fe4
 fe5
 fe6
 fe7
 fe8

域名	说明
选中网络接口	设置需要监控的物理网口，可以多选。
<input type="button" value="查看网口状态"/>	查看被监控网口状态

本界面中，点击 ，弹出以下界面：

监控网口	HA报警	监控结果
无记录		
<input type="button" value="关闭"/>		

菜单说明：

域名	说明
监控网口	正在监控的物理网口。
HA 报警	是否报警提示失效。
监控结果	显示通断状态。

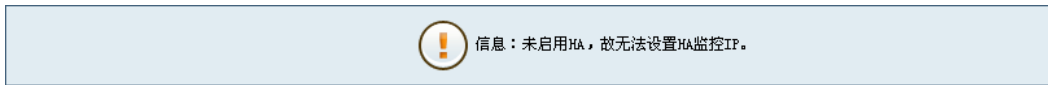
10.3. 高可用性>> HA 监控 IP

HA 路径监控对于用户了解 SLBP 集群中的安全网关设备连接状况是很有用的工

具，用它可以检查安全网关网络接口和其它设备接口之间的第 2 层和第 3 层网络连接是否有效。

监控周边设备 IP 属于第 3 层路径监控，IP 监控的功能是向指定的 IP 地址以固定的间隔发送 ARP 请求，然后监控目标是否响应。如果一个安全网关节点的监控 IP 总故障数超过该节点的故障切换临界值，则该安全网关节点将进入失效状态。当监控 IP 总故障数不再超过故障切换临界值后，它会从失效状态重新转变为有效状态。根据探测结果可以调整集群安全网关的失效状态，以便均衡负载。





如果没有启用 HA 功能，则在本页面显示如下信息：



如果启用了 HA 功能，本页面显示如下信息：

系统监控>>HA监控IP

如果监控周边设备IP列表中所有监控失败的IP的“权重”之和达到阈值 100 (1~100)，则置本防火墙为失效状态。


监控周边设备IP	权重	从该网口监控	操作
192.168.10.2	5	ge1	 
10.50.10.21	22	ge1	 

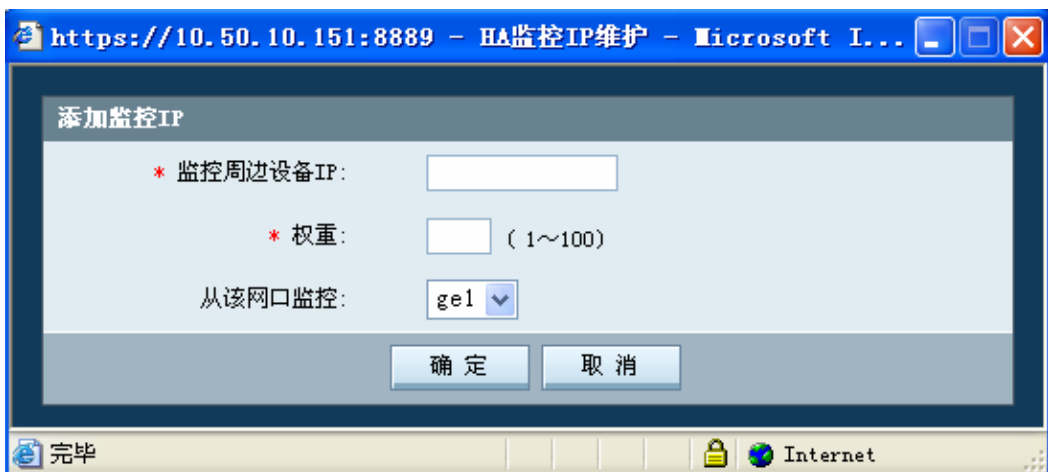
第1页/1页 跳转到 1 页 每页 20 行

菜单说明：

域 名	说 明
指定失效阈值	输入阈值，可以为 1-100 的整数 当监控的周边设备(如:路由器、交换机等)的权重之和达到该值， 则本节点将设置为失效状态，如果是双机热备的主安全网关，

	<p>则从安全网关立即接替其工作，如果是负载均衡中节点，其它节点将分担它的负载。</p> <p>点击“确定”后，设置生效。</p>
监控周边设备 IP	监控周边设备 IP。
权重	在所有监控周边设备中的权重。
从该网口监控	从哪个网口接口监控。
查看监控周边设备IP状态	查看监控周边设备 IP 状态。
操作	<p>添加、编辑、删除</p> <p>添加：添加新的监控周边设备 IP</p> <p>编辑：编辑本栏内容</p> <p>删除：删除本栏内容</p>

在“网络配置>>HA>>监控周边设备”界面中，点击 ，将弹出以下界面：



菜单说明：

域 名	说 明
监控周边设备 IP	监控周边设备 IP
权重	在所有监控周边设备中的权重
从该网口监控	从哪个网络接口监控

11. 用户认证

安全网关的用户认证主要被设计用于增强从内网访问外网时的控制。SecGate 3600-G10 安全网关的用户认证功能对用户的访问采用多层控制。通过对用户组的访问地址，访问服务，以及从哪里可以进行登录（即对源地址进行控制）来限制用户的访问，另外用户认证又是包过滤规则的一个子项，安全网关的包过滤规则又对访问进行了一层控制。

SecGate 3600-G10 安全网关支持本地用户认证和 RADIUS 认证功能，RADIUS 认证属于外部认证，安全网关此时作为 RADIUS 客户端，将内部用户传递来的信息转到 RADIUS 服务器上认证，然后将认证结果发回内部用户，这样安全网关上不必保存内部用户的各种信息，用户信息都保存在 RADIUS 服务器。

用户认证与“安全策略>>安全规则”配合使用。在安全规则（安全规则策略为“允许”或者“代理”）中选中“用户认证”，则应用该安全规则的连接必须先通过用户认证。

用户认证服务器，支持两种认证方式：

- （1）RADIUS 认证
- （2）本地认证



在“用户认证>>用户列表”和“用户认证>>用户组”界面中定义的用户和用户组

均设置在安全网关的本地用户认证库上。如果使用 RADIUS 认证方式，则用户的信息在 RADIUS 认证服务器上设置。

如果需要使用用户认证，必须定义用户库。在本地用户认证库中，提供了两种形式：

- (1) 用户：通常指单个人，如张三、李四等。
- (2) 用户组：通常指有共性的人，如同一个部门、同一种职位等。

注意

- (1) 用户可以不属于任何一个用户组：如刚来的新员工，还不属于任何一个部门。
- (2) 用户组中可以没有任何一个用户：如要成立一个新部门，还没有任何员工；又如，有一种职位，还没有任何员工。
- (3) 同一用户可以同时属于多个组：如一位员工，同时在 A 部门和 B 部门承担工作；又如，有一员工同时担任了多个职位。
- (4) 如果用户属性和组属性发生冲突，以用户属性为准。
- (5) 如果一个用户同时属于多个组，组之间的属性不同或者有冲突，取其最优值（大的，启用的，等等），不能累加。

【推荐】先定义用户组，再定义用户。

11.1. 用户认证>>服务器

为了增强从内网访问外网时的访问控制，提供不受服务种类限制的用户认证系统，可以为包过滤、双向 NAT、代理等访问控制提供用户认证功能。管理员可以启用安全

网关本地帐号服务器，也可以启用标准的 RADIUS 服务器。即，安全网关用户认证使用的是 RADIUS 的帐号库，并支持 RADIUS 服务器的审计功能。

用户认证>>服务器

用户认证服务器

*认证端口: (TCP)

*监控端口: (UDP)

本地帐号服务器

RADIUS服务器

IP地址:

认证端口: (默认:1812/UDP)

审计端口: (默认:1813/UDP)

密钥: (1-8位 字母、数字、减号、下划线的组合)

此界面包括以下功能：

1. 配置认证端口和监控端口
2. 选择认证服务器
3. 配置 RAUS 认证服务器

菜单说明：

域 名	说 明
认证端口	安全网关用户认证模块监听的认证端口 使用用户认证服务器，管理员必须配置认证端口和监控端口
监控端口	安全网关检测用户在线情况的监控端口 使用用户认证服务器，管理员必须配置认证端口和监控端口
本地帐号服务器	可以启用安全网关本地帐号服务器，也可以启用标准的 RADIUS 服务器。默认使用安全网关本地帐号服务器。

	<p>本地帐号服务器指安全网关上提供的用户认证服务器。本地帐号服务器可以提供更多的控制功能：</p> <ul style="list-style-type: none"> ✧ 提供基于角色的用户策略，并与安全规则策略配合完成强访问控制。主要包括：安全策略和授权服务。其中，安全策略是限制用户在什么时间、什么源 IP 地址可以登录安全网关系统，而授权服务则定义了该用户通过认证后能够享有的服务。 ✧ 支持对用户帐号的流量控制和时间控制 ✧ 客户端可以修改密码 ✧ 服务器端检查用户在线状态 ✧ 支持 PAP 和 S/Key 认证协议 <p>可以启用安全网关本地帐号服务器，也可以启用标准的 RADIUS 服务器。默认使用安全网关本地帐号服务器。</p>
RADIUS 认证服务器	启用 RADIUS 认证服务器，需要配置 RADIUS 认证服务器所在的 IP 地址、认证端口、审计端口及与安全网关加密通信的密钥
IP 地址	RADIUS 认证服务器所在的可以与安全网关通信的 IP 地址
认证端口	RADIUS 认证服务器的可以与安全网关通信的认证端口
审计端口	RADIUS 认证服务器的可以与安全网关通信的审计端口
密钥	RADIUS 认证服务器与安全网关加密通信的密钥

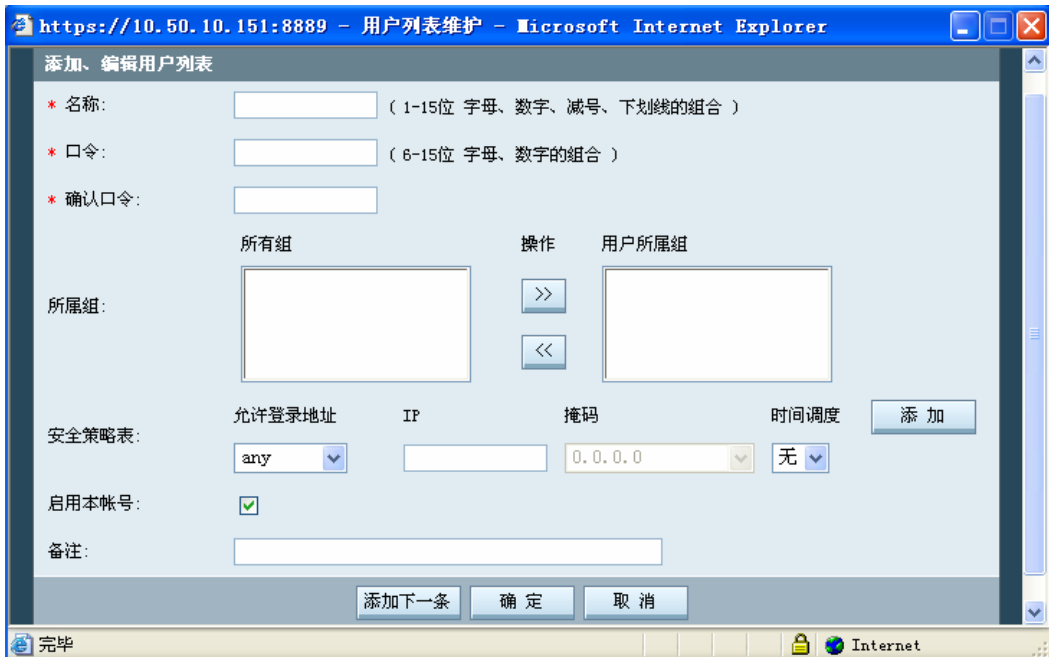
11.2. 用户认证>>用户列表

用户认证>>用户列表							请输入关键字	查找
序号	用户名	所属组	成功次数	失败次数	上次成功登录	备注	操作	
1	aaa		0	0	1970/01/01 08:00:00 0.0.0.0		 	
2	test		0	0	1970/01/01 08:00:00 0.0.0.0		 	

第1页/1页 跳转到 1 页 确定 每页 全部 行

可以按照用户名、登录成功次数、登录失败次数、上次成功登录时间和备注进行排序。

在“用户认证>>用户列表”界面中，点击 ，将弹出以下界面：



菜单说明：

值 域	说 明
名称	在用户、用户组中不能有相同的名称
口令	该用户用于认证的口令
所属组	左边的列表框列出了在“用户组”中定义的所有组 右边的列表框列出了本用户所属组 本用户所属组可以为空，即不属于任何组。
安全策略表	包括两项： 允许登录地址：指明该用户在指定的地址能够登录 时间调度：指明该用户只能在指定的时间段进行登录

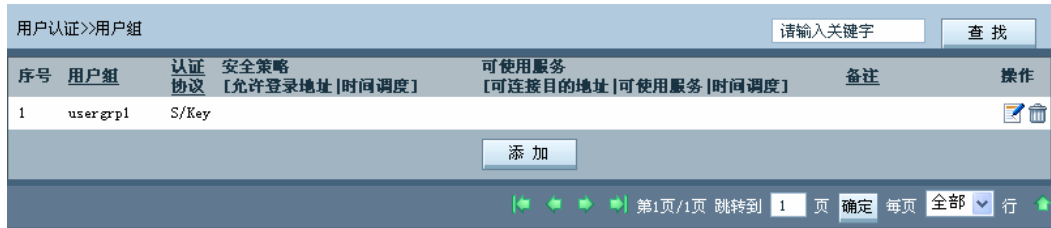
	<p>注意 如果在此处指定了安全策略，则以该用户的定义为准，而不使用该用户所属组的安全策略；如果此处没有指定安全策略，则使用所属组的安全策略，只要满足其中任何一个组的安全策略皆可登录。</p> <p>操作：</p> <p>添加：点击“添加”按钮</p> <p>删除：没有删除按钮，把该条策略的“允许登录地址”设为“删除该条”即可</p> <p>修改：直接点击列表进行修改即可</p>
启用本帐号	只有帐号启用后才能使用



在“用户认证>>用户列表”中，点击“编辑”，将弹出以下界面：



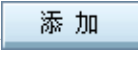
除可以针对原设置内容进行编辑外，还显示了用户帐号使用的状态信息。

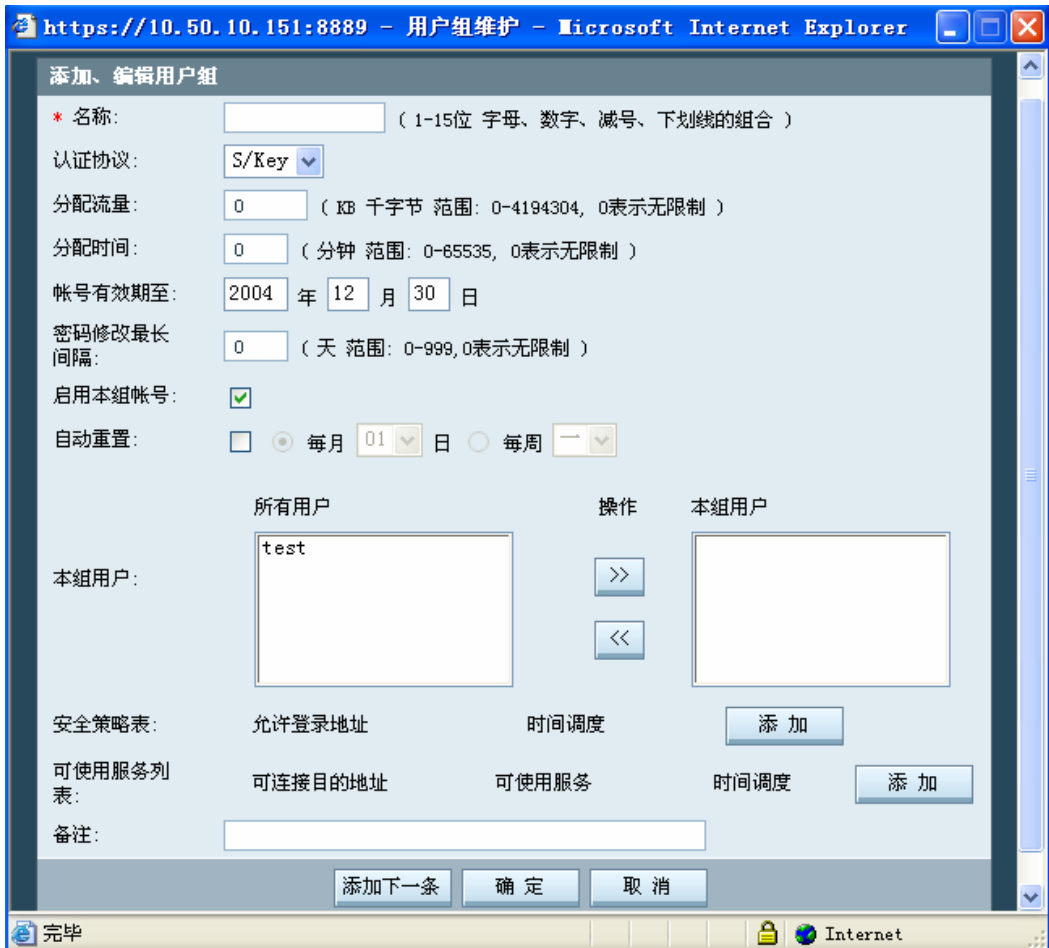
11.3. 用户认证>>用户组



序号	用户组	认证协议	安全策略 [允许登录地址 时间调度]	可使用服务 [可连接目的地址 可使用服务 时间调度]	备注	操作
1	usergrp1	S/Key				 

第1页/1页 跳转到 1 页 确定 每页 全部 行

在“用户认证>>用户组”界面中，点击 ，将弹出以下界面：



菜单说明：

值 域	说 明
名称	用户组名称。 在用户、用户组中不能有相同的名称
认证协议	SKEY：一次性认证口令，可以通过网御神州电子钥匙认证

	PAP: 用普通的口令进行认证
分配流量	<p>给该用户组中每个用户帐号分配的流量</p> <p>分配流量使用完毕后用户帐号自动锁定, 重置后才能恢复使用</p> <p>注意 如果用户认证已通过, 但访问不能成功, 可以检查一下当前可用流量是否够当前访问所需的字节数。</p>
分配时间	<p>给该用户组中每个用户帐号分配的时间</p> <p>分配时间使用完毕后用户帐号自动锁定, 重置后才能恢复使用</p>
帐号有效期至	用户帐号在此日期以前有效, 过期则失效, 需重新设定有效期才能生效
密码修改最长间隔	<p>口令使用一段时间以后, 最好能定期更新, 为培养良好的口令更新习惯。如果超过了最长修改间隔(如: 10 天)未修改密码, 则登录时客户端告警客户, 建议其最好修改密码。</p> <p>为空表示无限制, 不做告警。</p>
启用本组帐号	<p>选中则启用本组帐号, 否则禁用本组帐号</p> <p>“用户”设置中也有该属性, 当有冲突时, 以用户设置的属性为准。</p>
自动重置	<p>选中则定期重置“分配流量”和“分配时间”, 恢复被锁定的帐号</p> <p>有两种方式: 每月重置或者每周重置</p> <p>如: 用户组“GrpA”分配流量为 15000K, 每月 1 号自动重置,</p>

	<p>用户“A1”属于用户组“GrpA”。用户“A1”在25号共计使用了15000K流量，可用流量还剩0，则帐号自动被锁定，到下月1号，用户“A1”帐号解除锁定，可用流量重新被置为15000K。</p>
<p>本组用户</p>	<p>左边的列表框列出了在“用户认证>>用户列表”中定义的所有用户。</p> <p>右边的列表框列出了属于本组的用户</p> <p>被添加到“本组用户”列表的用户将不再显示于“所有用户”列表中。</p> <p>用户组可以无任何成员</p>
<p>安全策略表</p>	<p>包括两项：</p> <p>允许登录地址：指明该组所有用户在指定的地址进行登录</p> <p>时间调度：指明该用户在指定的时间段能够登录</p> <p>注意 如果用户指定了安全策略，则忽略其所属组的策略，仅用户处指定的策略有效。如果用户处未指定安全策略，则只要满足其所属组的任何一条安全策略，用户都可以通过认证。</p> <p>操作：</p> <p>添加：点击“添加”按钮</p> <p>删除：没有删除按钮，把该条策略的“允许登录地址”设为“删</p>

	<p>除该条”即可</p> <p>修改：直接点击列表进行修改即可</p>
可使用服务列表	<p>指定该组用户帐号通过认证后可以使用的服务。</p> <p>包括三项：</p> <p>可连接目的地址：通过认证后可连接的目的地址。下拉框中显示的内容为在“对象定义>>地址>>地址列表”和“对象定义>>地址>>地址组”中定义的所有地址和地址组。</p> <p>可使用服务：通过认证后用户可使用的服务。下拉框中显示的内容为在“对象定义>>服务>>服务列表”和“对象定义>>服务>>服务组”中定义的所有服务和组。</p> <p>时间调度：通过认证后可以使用服务的时间端。下拉框中显示的内容为在“对象定义>>时间>>时间列表”和“对象定义>>时间>>时间组”中定义的所有时间和时间组。</p>

12. 系统监控

安全网关运行中，管理员需要监控安全网关所在网络以及安全网关本身的运行状态。

SecGate 3600—G10 安全网关提供了两种监控方式：

(1) 通过安全网关配置管理界面直接监控：可以监控 HA 状态、日志信息、资源状态、网络接口、在线用户等。由于安全网关本地资源有限，只保存有限的监控信息，且只能监控单台安全网关。

(2) 安装 SecGate 3600—G10 安全网关配套的 SecGateManager 集中管理系统：该软件安装在集中管理主机上，根据软件版本、安装配置情况，可以监控多台安全网关，并保留更多的监控信息，提供详细查询及报表等功能。

安全网关监控信息包括：

- (1) HA 状态：在主节点上可以监控所有节点的状态。
- (2) 日志信息：对日志简单分类和过滤
- (3) 资源状态：CPU 利用率、内存利用率
- (4) 网络接口状态：网口的实时状态和流入、流出量的统计信息
- (5) VPN 隧道监控
- (6) DHCP 用户信息
- (7) 在线用户：当前通过用户认证功能的在线用户的信息

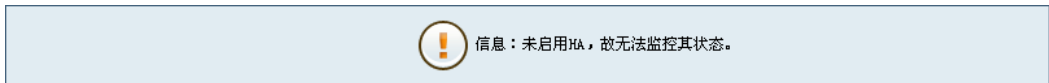
- (8) 在线管理员：查看当前管理安全网关的管理员信息
- (9) ARP 表：系统内部 ARP 表的状态
- (10) IP 诊断：提供一些基本的调试工具 ping 和 traceroute



安全网关上当前的状态信息和统计信息在断电后不保存。

12.1. HA 状态

如果没有启用 HA 功能，则在本页面显示如下信息：



如果启用了 HA 功能，可以在本页面监控 HA 状态。如下图所示：

系统监控>>HA状态				
节点号	优先级	HA网口IP地址	配置同步状况	详细状态
1	1	192.168.10.1	已同步	详细

显示该 HA 节点当前的 IP、ID、优先级、配置同步状况及其详细信息。

12.2. 日志信息

安全网关提供包过滤、代理、双向 NAT、配置管理等功能模块的日志信息。

安全网关日志信息有两种处理方式：

(1) 安全网关本地保留日志：默认方式。以原始日志格式显示，最多保存 2M 大小的日志信息，安全网关断电后本地日志不保存。查询只能按日志类型、日志级别和关键词进行查找。

(2) 发送给日志服务器处理：如果使用集中管理系统的日志审计软件（需要安装一台日志服务器，可以直接安装在集中管理主机上），可以对安全网关日志原始日志进行详细解析，并提供详细查询、统计、报表功能，根据日志服务器磁盘空间大小可以保存数量庞大的日志信息。



推荐使用日志服务器来接收、保存、查询、统计日志信息。

日期/时间	级别	详细信息
2006/02/15 15:19:03	信息	Feb 15 15:19:03 firewall webui: devid=0 date="2006/02/15 15:19:03" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.10 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="homepage"
2006/02/15 15:18:59	信息	Feb 15 15:18:59 firewall webui: devid=0 date="2006/02/15 15:18:59" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.23 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="log"
2006/02/15 15:18:56	信息	Feb 15 15:18:56 firewall webui: devid=0 date="2006/02/15 15:18:56" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.23 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="log"
2006/02/15 15:18:52	信息	Feb 15 15:18:52 firewall webui: devid=0 date="2006/02/15 15:18:52" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.23 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="log"
2006/02/15 15:18:48	信息	Feb 15 15:18:48 firewall webui: devid=0 date="2006/02/15 15:18:48" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.23 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="log"
2006/02/15 15:18:38	信息	Feb 15 15:18:38 firewall webui: devid=0 date="2006/02/15 15:18:38" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.23 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="log"
2006/02/15 15:18:33	信息	Feb 15 15:18:33 firewall webui: devid=0 date="2006/02/15 15:18:33" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.10 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="homepage"
2006/02/15 15:18:32	信息	Feb 15 15:18:32 firewall webui: devid=0 date="2006/02/15 15:18:32" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.23 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="log"
2006/02/15 15:18:28	信息	Feb 15 15:18:28 firewall webui: devid=0 date="2006/02/15 15:18:28" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.23 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="log"
2006/02/15 15:18:23	信息	Feb 15 15:18:23 firewall webui: devid=0 date="2006/02/15 15:18:23" dname=firewall logtype=9 pri=6 mod=webui from=10.50.10.23 agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" act=show page="log"

第1页/32页 跳转到 页 确定 每页 10 行

- 日志类型：
- 安全规则
 - 代理
 - 入侵检测
 - 抗攻击
 - VPN
 - 用户认证
 - 内容过滤
 - 设备状态
 - 设备管理**
 - HA
 - 其他
 - 所有

日志类型包括：


- 日志级别：
- 所有**
 - 警报
 - 紧急
 - 一般
 - 临界
 - 事件
 - 错误
 - 警告
 - 注意
 - 信息
 - 调试

日志级别包括：

日志类型	描 述
包过滤日志	包过滤（包括：包过滤、NAT、IP 映射、端口映射、代理、抗攻击日志等）
代理日志	HTTP/FTP/TELNET/SMTP/POP3 代理的日志，不包括其内容过滤的日志
入侵检测日志	IDS 联动的日志（ 注意 IDS 本身的日志只记录在 IDS 系统中，不记录到安全网关上。）
抗攻击日志	所有抗攻击功能启用的日志
VPN 日志	VPN 相关日志信息，隧道建立相关状态信息
用户认证日志	用户认证模块的日志
内容过滤	POP3/SMTP 邮件内容过滤的日志
设备状态日志	设备运行状况的日志，包括设备状态被修改的日志
设备管理日志	管理员操作日志，主要指界面操作日志（WEB 和 CLI）
HA	HA 模块记录的日志
其他	其他所有模块记录的日志
级 别	说 明
所有	所有日志
警报	包括紧急、一般、和临界警报
紧急	紧急警报，导致系统不可用的事件消息
一般	一般警报，应立即采取应对行动的事件消息

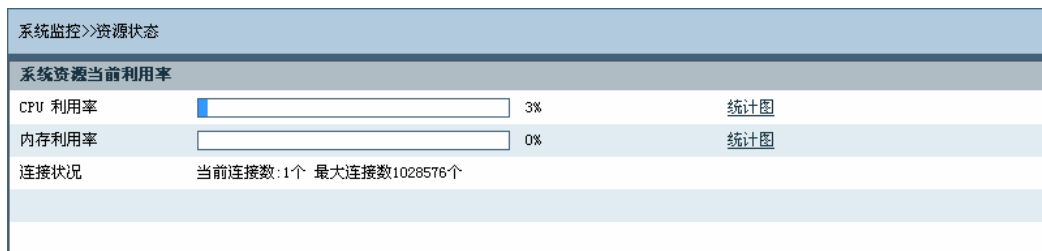
临界	临界警报，达到临界条件的事件消息
事件	包括错误、警告、注意、信息、和调试事件
错误	错误事件，一般出错事件消息
警告	警告事件，预警性提示事件消息
注意	注意事件，重要的正常事件消息
信息	信息事件，一般性的正常事件消息
调试	调试事件，调试消息



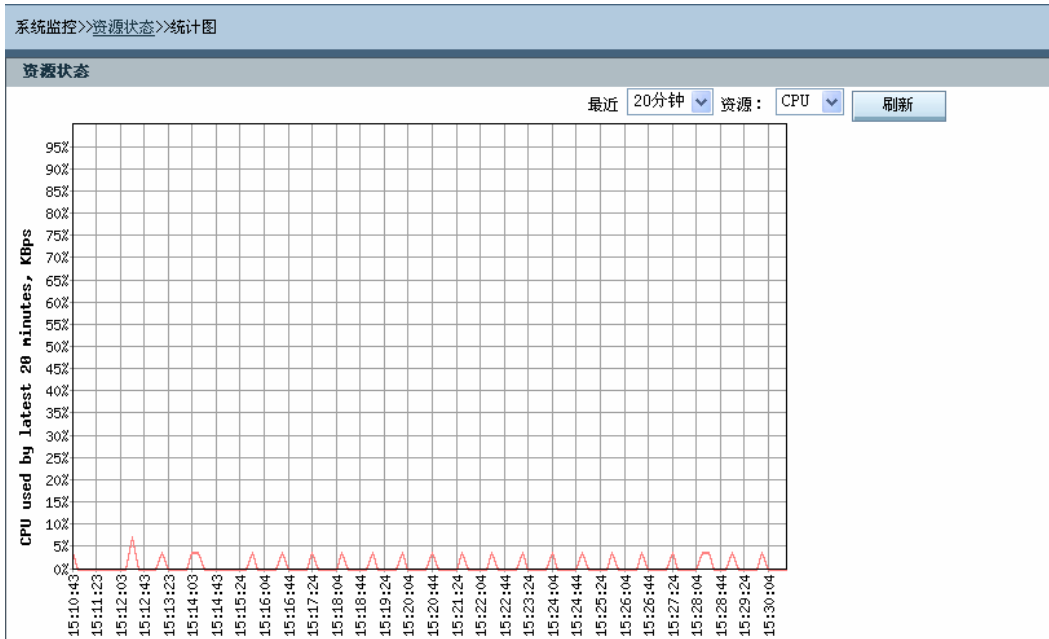
- (1) 选中类型和级别后，需要点击  才进行查找。
- (2) 如果关键词输入框中有内容，则同时按关键词进行查找，如果没有内容，则不按关键词查找。

12.3. 资源状态

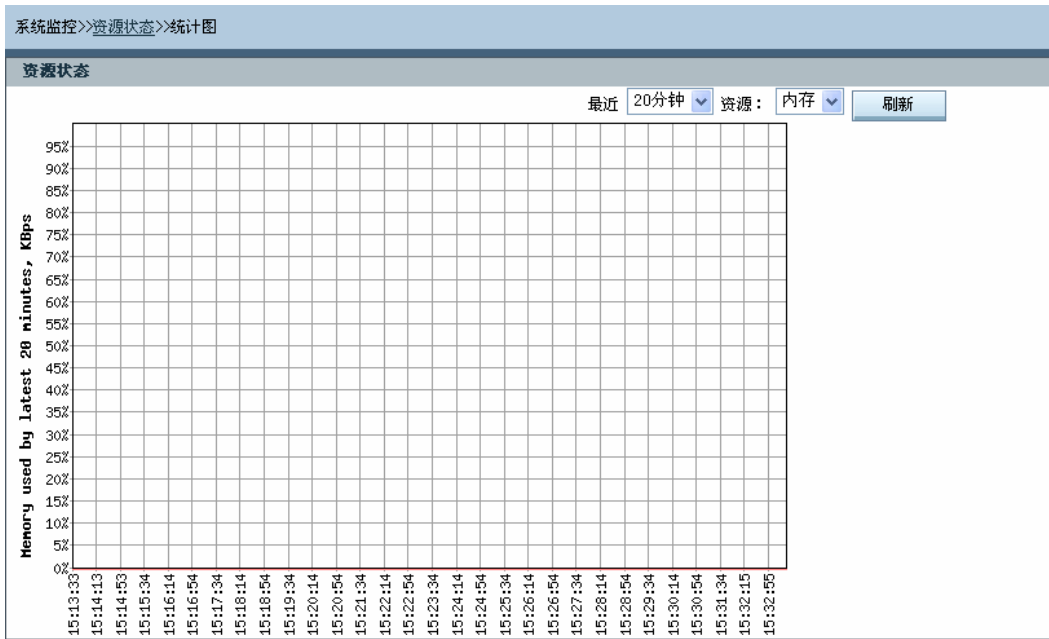
显示当前 CPU 和内存的利用率。



统计图（CPU）显示 CPU 已使用的统计信息，如下图所示：



统计图（内存）显示内存已使用的统计信息，如下图所示：



12.4. 网络接口

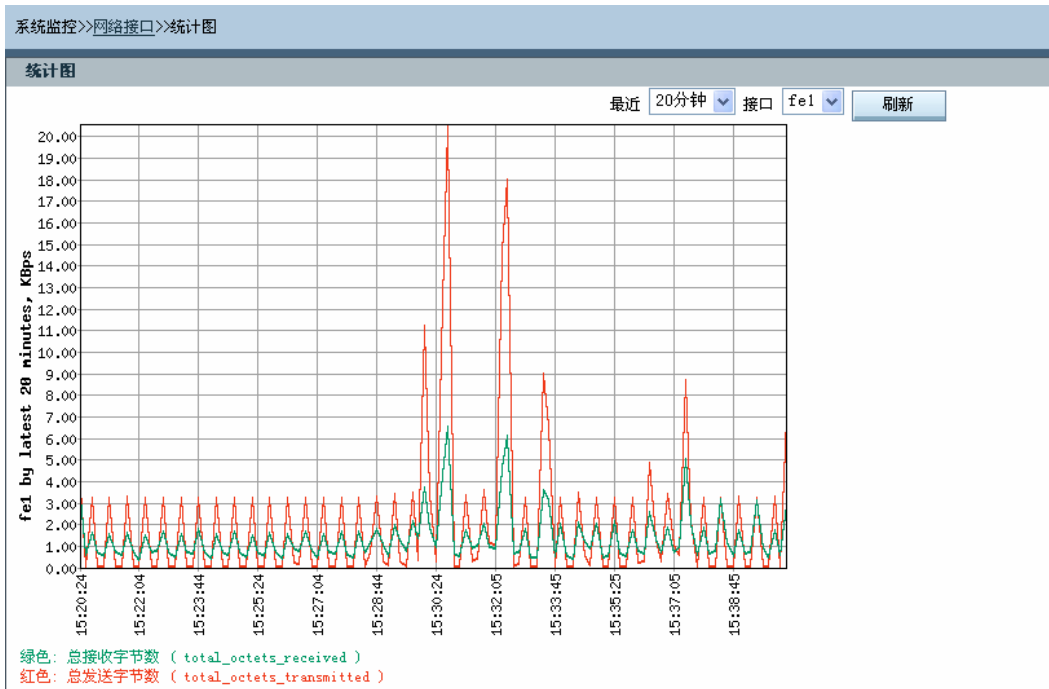
网络接口显示所有已激活网口的当前通断状态和流量统计信息，如下图所示：

系统监控>>网络接口					
网络接口	状态	流量			
ge1		发送 72050	接收 68518	当前状态	统计图
ge2		发送 0	接收 0	当前状态	统计图
ge3		发送 0	接收 0	当前状态	统计图
fe1		发送 12290504	接收 12914276	当前状态	统计图
fe2		发送 0	接收 0	当前状态	统计图
fe3		发送 0	接收 0	当前状态	统计图
fe4		发送 0	接收 0	当前状态	统计图
fe5		发送 0	接收 0	当前状态	统计图
fe6		发送 0	接收 0	当前状态	统计图
fe7		发送 0	接收 0	当前状态	统计图
fe8		发送 0	接收 0	当前状态	统计图

当前状态显示了网络接口当前流量的详细信息，如下图所示：

系统监控>>网络接口>>当前状态						
					接口： <input type="text" value="ge1"/>	<input type="button" value="刷新"/>
网络接口 ge1 当前接收状态						
Short Frames	0	Fragments	0	Frames Received (64 Octets)	73	
Frames Received (65 to 127 Octets)	1	Frames Received (128 to 255 Octets)	284	Frames Received (256 to 511 Octets)	0	
Frames Received (512 to 1023 Octets)	0	Frames Received (1024 to 1518 Octets)	0	Long Frames Received	0	
Jabber	0	Frames with Bad CRC	0	Unicast Frames Received	358	
Broadcast Frames Received	0	Multicast Frames Received	0	Total Frames Received	358	
Receive Errors	0	Pause Frames	0	Total Pause Time	0	
Total Octets Received	68518	Overruns	0	Jumbo Frames	0	
网络接口 ge1 当前发送状态						
Short Frames	0	Runt Frames	0	Frames Transmitted (64 Octets)	0	
Frames Transmitted (65 to 127 Octets)	310	Frames Transmitted (128 to 255 Octets)	0	Frames Transmitted (256 to 511 Octets)	0	
Frames Transmitted (512 to 1023 Octets)	0	Frames Transmitted (1024 to 1518 Octets)	48	Long Frames Transmitted	0	
Jabber	0	Late Collisions	0	Total Collisions	0	
Single Collisions	0	Multiple Collisions	0	Excessive Deferrals	0	
Transmit Underruns	0	CRC Errors	0	Excessive Collisions	0	
Unicast Frames Transmitted	22	Broadcast Frames Transmitted	0	Multicast Frames Transmitted	336	
Total Octets Transmitted	72050	Jumbo Frames Transmitted	0	Aborted Frames	0	
Total Frames Transmitted	358					

统计图显示了各个网络接口的总接收字节数和总发送字节数。如下图所示：



12.5. VPN 隧道监控

该页面将列出所有已建立的隧道，用户可以看到这些隧道的状态信息。

系统监控 >> VPN隧道监控

请输入关键字 查找

隧道名	远程地址	状态	源地址	远程身份	创建时间	生存周期	算法
zhang	10.50.10.10	established	1.1.1.3/32	zhang	2006/2/15 17:18:54	1800	3des-md5

刷新

第1页/1页 跳转到 1 页 确定 每页 全部 行

菜单说明:

域 名	说 明
-----	-----

域 名	说 明
隧道名	隧道名称，唯一标识，符合命名规则
远程地址	远程 VPN 端点的 IP 地址
状态	该隧道的状态
源地址	远程 VPN 的内部地址
远程身份	远程 VPN 的身份
创建时间	隧道建立的时间
生存周期	隧道的密钥生存周期
算法	隧道保护数据用到的算法

12.6. DHCP 用户信息

可以监控安全网关做为 DHCP 服务器时 DHCP 用户的相关信息。

系统监控>>DHCP用户信息					
主机名	IP地址	子网掩码	MAC地址	租期开始时间	租期结束时间
无 记 录					
<input type="button" value="刷新"/>					

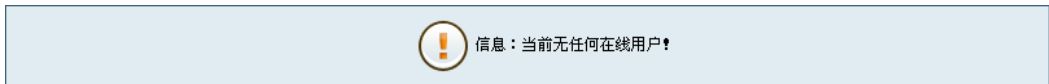
数据域说明：

域 名	说 明
主机名	DHCP 客户端的主机名
IP 地址	DHCP 客户端获取到的 IP 地址

域 名	说 明
子网掩码	DHCP 客户端获取到的子网掩码
MAC 地址	DHCP 的 MAC 地址
租用开始时间	租用 DHCP 地址的起始时间
租用结束时间	租用 DHCP 地址的结束时间

12.7. 在线用户

如果没有使用用户认证功能，则在本页面显示如下信息：



如果使用了用户认证功能，可以在本页面监控所有在线用户。

可以监控的信息包括：用户名、登录 IP、登录时间、在线时长，流入流量和流出流量。如下图所示：

系统监控>>在线用户						
序号	用户名	登录IP	登录时间	在线时长	流入流量 (KB)	流出流量 (KB)
<input type="checkbox"/> 1	test	10.50.10.21	2006/02/16 16:58:57	0:00:05	0	0
<input type="checkbox"/> 全选				<input type="button" value="中断"/>	<input type="button" value="刷新"/>	

管理员可以强制中断在线用户。中断某用户操作步骤如下：

- 选中待删除用户对应的复选框 1
- 点击 ，即可中断该用户的连接。

被中断的用户端会收到服务器断开连接的提示。只有重新登录，该用户才能使用

只有在用户认证允许的服务。



- (1) 管理员修改了用户策略，只有用户重新登录时才能生效。
- (2) 系统每 100 秒更新一次在线用户的监控信息，因此，从该界面上看到的监控信息实际上是上一次更新时的实际数据。

12.8. 在线管理员

在本页面显示所有在线管理员。显示的信息包括：管理员名称、登录方式、登录地点、登录时间。如下图所示：

管理员名称	登录方式	登录地点	登录时间
administrator	WEB	10.50.10.27	2005/09/11 16:17:59

点击 ，可以显示当前时刻所有在线管理员的信息。

12.9. ARP 表

显示安全网关当前的 ARP 表

序号	IP地址	MAC地址	网络接口	标志位
1	10.50.10.27	00:0F:EA:EB:BA:CD	fe1	C
2	10.50.10.215	00:0C:29:57:0E:B1	fe1	C

值 域	说 明
-----	-----

IP 地址	列出 IP 地址
MAC 地址	列出 MAC 地址
网络接口	该 ARP 所对应的安全网关接口
清空 ARP 表	将安全网关当前 ARP 全部清空
全部设置为静态 ARP	将安全网关当前 ARP 全部设置为静态方式。  重启安全网关以后，这些静态 ARP 将丢失，不能保存到系统中。

12.10.IP 诊断

IP 诊断是用于判断与安全网关相连的网络是否通畅。



IP地址:

输入需要诊断的 IP 地址，点击“Ping”，下图的诊断结果显示：从安全网关能 ping 通 10.50.10.1

系统监控>>IP诊断>>诊断结果

```
PING 10.50.10.1 (10.50.10.1) from 10.50.10.230 : 56(84) bytes of data.  
64 bytes from 10.50.10.1: icmp_seq=0 ttl=128 time=998.080 msec  
64 bytes from 10.50.10.1: icmp_seq=1 ttl=128 time=187 usec  
64 bytes from 10.50.10.1: icmp_seq=2 ttl=128 time=173 usec  
64 bytes from 10.50.10.1: icmp_seq=3 ttl=128 time=184 usec  
64 bytes from 10.50.10.1: icmp_seq=4 ttl=128 time=184 usec  
  
--- 10.50.10.1 ping statistics ---  
5 packets transmitted, 5 packets received, 0% packet loss  
round-trip min/avg/max/mdev = 0.173/199.761/998.080/399.159 ms
```

[返回](#)

下图的诊断结果显示，从安全网关不能 ping 通 10.50.10.230

系统监控>>IP诊断>>诊断结果

```
PING 10.50.10.232 (10.50.10.232) from 10.50.10.230 : 56(84) bytes of  
data.  
From 10.50.10.230: Destination Host Unreachable  
From 10.50.10.230: Destination Host Unreachable  
From 10.50.10.230: Destination Host Unreachable  
From 10.50.10.230: Destination Host Unreachable  
  
--- 10.50.10.232 ping statistics ---  
5 packets transmitted, 0 packets received, +4 errors, 100% packet loss
```

[返回](#)

如果用 Traceroute 诊断 IP，则如下图显示：

系统监控>>IP诊断>>诊断结果

```
traceroute to 10.50.10.1 (10.50.10.1), 30 hops max, 38 byte packets  
1 server.secuward.com (10.50.10.1) 0.412 ms 0.199 ms 0.168 ms
```

[返回](#)

附录一 用户认证客户端软件安装使用指南

1.概述

用户认证客户端程序主要有如下两个功能：

1. 认证功能：用户通过该软件向认证服务器提出认证请求。在认证通过后，用户就可以使用需要认证才能使用的网络服务，
2. 修改口令：用户通过该软件可以在登录成功后，修改自己帐号的口令。

本程序支持使用电子钥匙。如果使用电子钥匙，认证服务器的地址和认证端口，以及用户认证时的帐号和密码将存储的电子钥匙上；否则，认证服务器的地址和认证端口存放在系统配置中，用户登录时输入帐号和密码。如果需要修改密码，则在认证前程序会提示用户输入新密码。软件支持 **SKEY** 和 **PAP** 两种认证协议，并能自动使用一种进行认证。

认证通过后，认证服务器将该用户当前 **IP** 添加到认证 **IP** 列表中，从而用户可以使用那些需要认证后才能使用的网络功能。用户在使用网络的过程中，不能关闭该程序，否则，用户 **IP** 将被从认证 **IP** 列表中删除，将不能继续使用那些需要认证才能使用的网络功能。

如果采用电子钥匙方式，则在使用过程中，电子钥匙不能拔出，否则，系统会自动断开连接。

2. 客户端软件的安装

请您先运行 AuthClientInstall.exe，然后按提示进行操作。

3. 基本使用方法

3.1 客户端主界面

启动程序后，将看到如下窗口



图 1 主界面

无论用户是否使用电子钥匙，用户第一次启动本程序时，都是看到图 1 的主界面。但是，本节后面的介绍都是指在不使用电子钥匙的情况下。

3.2 配置系统

点击“设置>>服务器配置”按钮，可以配置本程序。各选择项的含义解释如下。



图 2 配置客户端

服务器地址：认证服务器的 IP 地址（一般是与本机连接的安全网关网口的 IP 地址）；

端口号：认证服务器提供认证服务的端口号；

3.3 认证

在配置界面中设置好正确的服务器地址和端口后，点击“确定”，返回到程序的主界面（如图 1 所示）。然后输入正确的用户名和密码后，点击“连接”按钮，开始进行认证；此时，窗口上红灯变为黄灯，界面变为：



图 3 处于认证过程中的界面

在通过认证后，应看到图 4

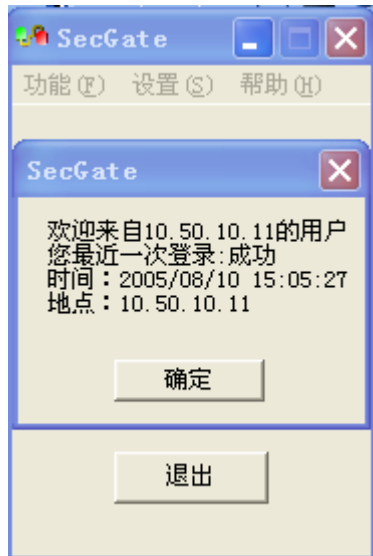


图 4 认证通过

3.4 修改密码

认证成功后，将出现修改密码的按钮，此时，用户可以修改密码。

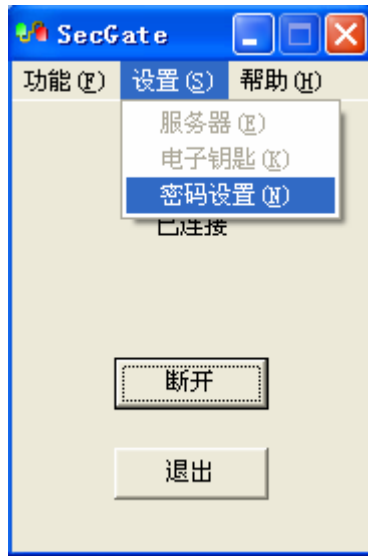


图 5 点击修改密码的按钮



图 6 输入新密码

在输入新密码后，请按“确定”，开始进行认证并修改密码。如果修改成功，可以看到如下图所示：



图 7 成功修改密码

4. 电子钥匙的使用方法

4.1 电子钥匙驱动程序的安装

请参阅《网御神州 SecGate 3600-G10 安全网关快速指南》中的相关部分。

4.2 配置电子钥匙

在主界面（见图 1）中，点击“设置>>电子钥匙”，弹出窗口：



配置电子钥匙	
电子钥匙参数设置	
服务器地址	10.50.10.213
端口号	9998
用户名	user1
密码	*****
重输密码	*****
读取 写入 更改PIN>> 退出	

图 8 配置电子钥匙

请在其中填写相应内容后，点击“写入”按钮。此时，将会要求您输入电子钥匙的 PIN：



PIN密码校验	
PIN密码	*****
确认 取消	

图 9 电子钥匙 PIN 校验

请输入正确 PIN 后点击“确认”，如果写操作成功，将看到：

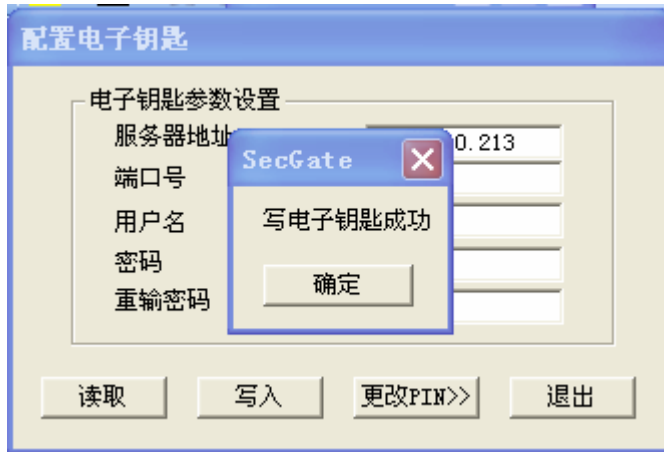


图 10 写电子钥匙成功

4.3 修改电子钥匙 PIN 口令

在配置电子钥匙的窗口中，点击“更改 PIN”，可以更改电子钥匙的 PIN。如下图所示：

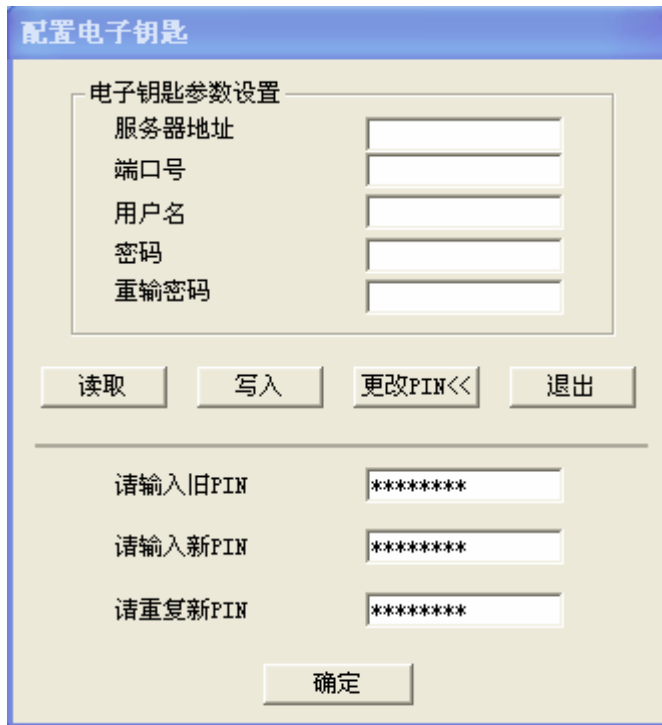


图 11 修改电子钥匙 PIN

4.4 认证

使用电子钥匙时，登录界面变为



图 12 使用电子钥匙时的登录界面

由于不需要用户输入帐号和密码(均可从电子钥匙中获取),所以这两个输入框都变为只读,且用户名固定显示为 ltoken。

点击“连接”即可开始认证。如果此前电子钥匙的 PIN 没有被检验过,则会要求用户输入电子钥匙的 PIN。认证成功后,系统界面变为:



图 13 使用电子钥匙时的认证通过界面

4.5 修改口令

与不使用电子钥匙时的修改方法基本一样，所不同的是，系统还将同时更新电子钥匙里存储的密码，所以，请您千万不要拔出电子钥匙。

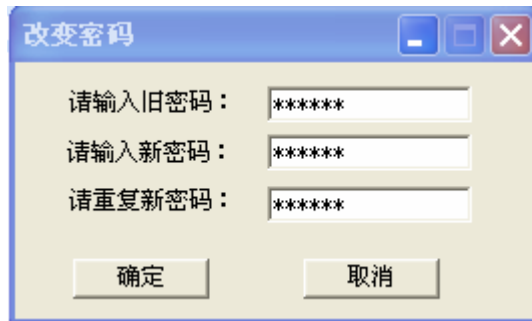


图 14 使用电子钥匙时修改密码