SMP.edu Pro

—

618 19 -22

350002

http://www.ruijie.com.cn

http://support.ruijie.com.cn

4008-111-000

E-mail: service@ruijie.com.cn

RGOS® RGNOS®

1

RG-SMP

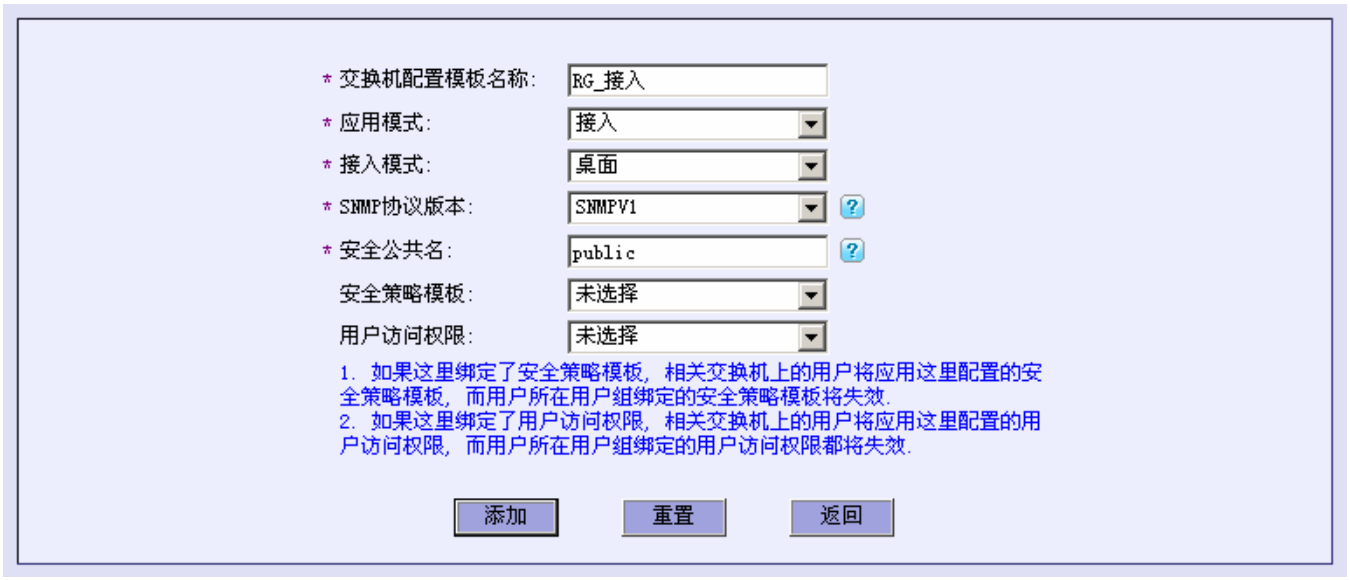
- SAM
-
-
-
-
-
-
-
-
- ARP

1.1 SAM

SAM SAM RG-SMP

1.1.1

“ ” “ ”


* 交换机配置模板名称: RG_接入
* 应用模式: 接入
* 接入模式: 桌面
* SNMP协议版本: SNMPV1
* 安全公共名: public
安全策略模板: 未选择
用户访问权限: 未选择
1. 如果这里绑定了安全策略模板，相关交换机上的用户将应用这里配置的安全策略模板，而用户所在用户组绑定的安全策略模板将失效.
2. 如果这里绑定了用户访问权限，相关交换机上的用户将应用这里配置的用户访问权限，而用户所在用户组绑定的用户访问权限都将失效.
添加
重置
返回

“ ”

1.1.2

“ ” “ ”

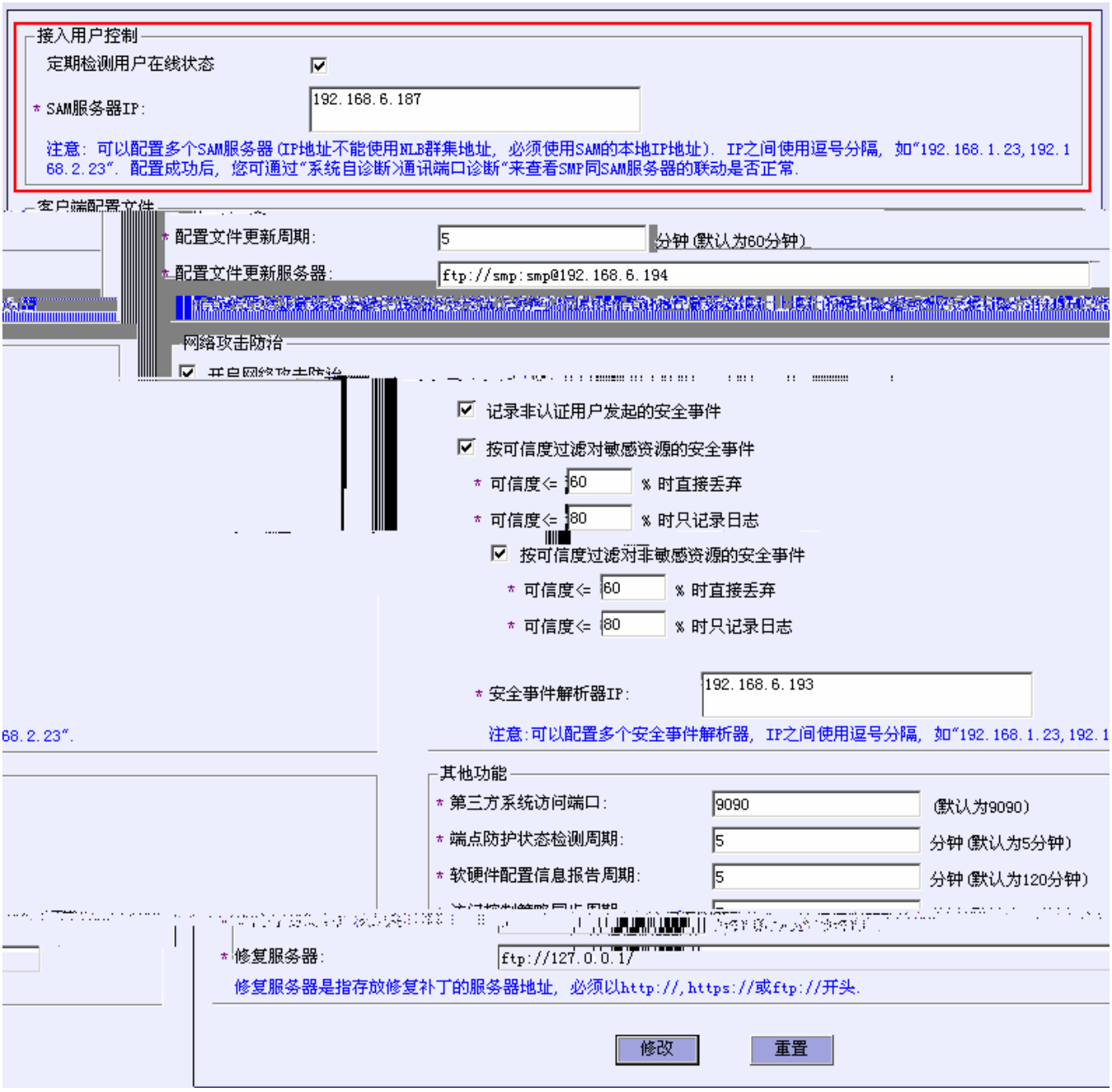
IP

SMP

“ ”

1.1.3

“ ” “ ” SAM


接入用户控制
定期检测用户在线状态
* SAM服务器IP:
192.168.6.187
注意：可以配置多个SAM服务器(IP地址不能使用NLB群集地址，必须使用SAM的本地IP地址)，IP之间使用逗号分隔，如"192.168.1.23,192.168.2.23"。配置成功后，您可通过"系统自诊断>通讯端口诊断"来查看SMP同SAM服务器的联动是否正常。
客户端配置文件
* 配置文件更新周期:
5
分钟(默认为60分钟)
* 配置文件更新服务器:
ftp://smp:smp@192.168.6.194
网络攻击防治
记录非认证用户发起的安全事件
按可信度过滤对敏感资源的安全事件
* 可信度<= 60 % 时直接丢弃
* 可信度<= 80 % 时只记录日志
按可信度过滤对非敏感资源的安全事件
* 可信度<= 60 % 时直接丢弃
* 可信度<= 80 % 时只记录日志
* 安全事件解析器IP:
192.168.6.193
注意:可以配置多个安全事件解析器，IP之间使用逗号分隔，如"192.168.1.23,192.1
68.2.23"。
其他功能
* 第三方系统访问端口:
9090
(默认为9090)
* 端点防护状态检测周期:
5
分钟(默认为5分钟)
* 软硬件配置信息报告周期:
5
分钟(默认为120分钟)
* 修复服务器:
ftp://127.0.0.1/
修复服务器是指存放修复补丁的服务器地址，必须以http://,https://或ftp://开头。
修改
重置

“ ”

1.2

RG-SMP

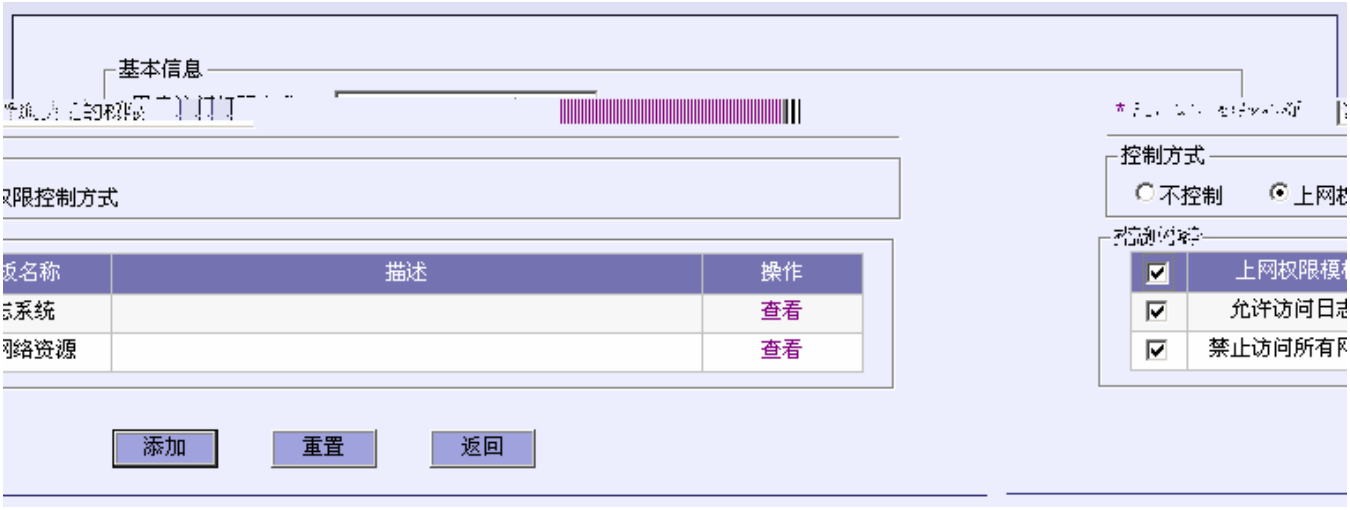
1.2.1

1.1

1.2.2

“ ” “ ”

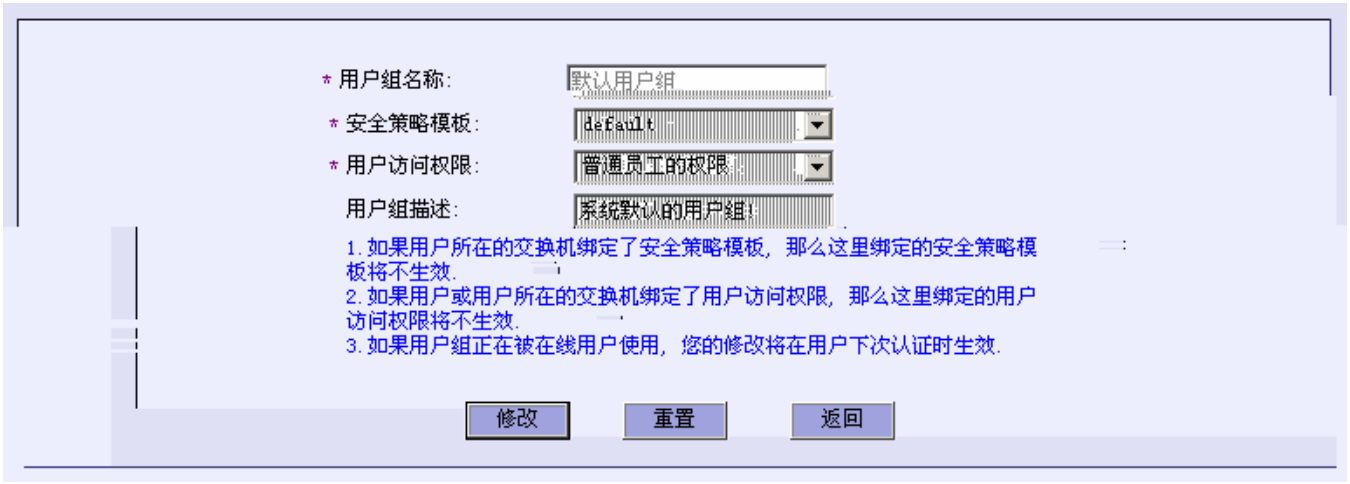
“ ”



“ ”

1.2.3

“ ”



“ ”

1.3

RG-SMP PC

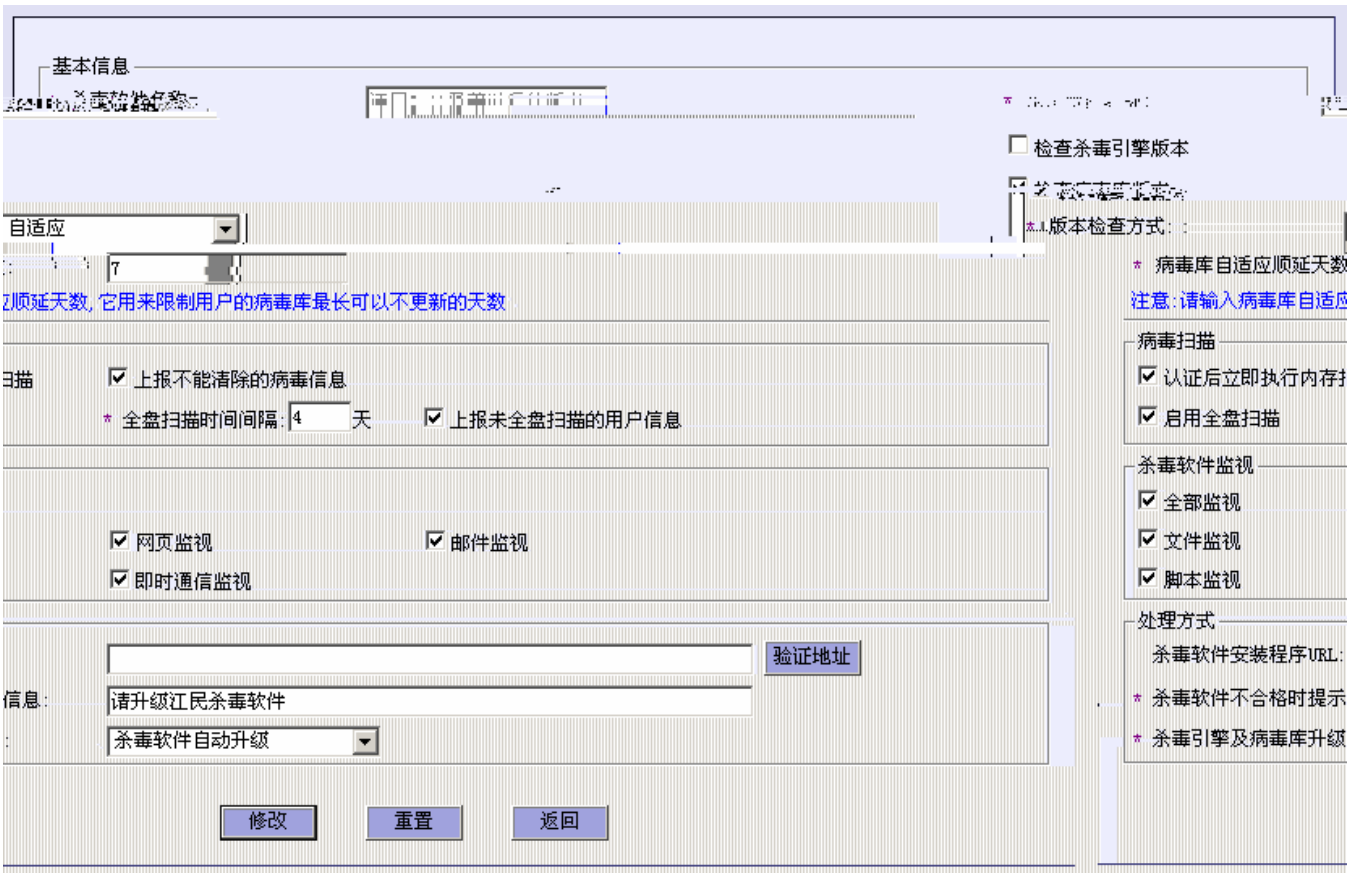
1.3.1

1.1

1.3.2

“ ”


杀毒软件名称
联动方式
检查项
检查限制
启用
操作
检查
自适应顺延天数
7
查看 修改
不检查
检查
自适应顺延天数
7
查看 修改
江民杀毒软件KV2007
弱联动
杀毒引擎
病毒库
查看 修改
不支持
检查
自适应顺延天数
7
查看 修改
卡巴斯基互联网安全套装6.0个人版
弱联动
查看 修改
不支持
检查
自适应顺延天数
7
查看 修改
卡巴斯基反病毒7.0个人版
弱联动
杀毒引擎
不检查
病毒库
检查
自适应顺延天数
7
查看 修改
Symantec AntiVirus企业版 8
弱联动
杀毒引擎
不检查
查看 修改
Symantec AntiVirus企业版 9
弱联动
7
查看 修改
Symantec AntiVirus企业版 10
弱联动
杀毒引擎
不检查
7
查看 修改
安博士杀毒软件 V3 VirusBlock2005
弱联动
杀毒引擎
检查
自适应顺延天数
病毒库
不支持
查看 修改
McAfee VirusScan V10.0
弱联动
杀毒引擎
不检查
病毒库
不检查
查看 修改
McAfee VirusScan Enterprise 8.5.0i
弱联动
杀毒引擎
不检查
病毒库
不检查
7
查看 修改
NOD32 2.5
弱联动
杀毒引擎
不支持
病毒库
检查
自适应顺延天数
7
查看 修改
NOD32 2.7
弱联动
杀毒引擎
不支持
病毒库
检查
自适应顺延天数


基本信息
检查杀毒引擎版本
自适应
7
顺延天数，它用来限制用户的病毒库最长可以不更新的天数
上报不能清除的病毒信息
全盘扫描时间间隔: 4 天
上报未全盘扫描的用户信息
网页监视
邮件监视
即时通信监视
验证地址
请升级江民杀毒软件
杀毒软件自动升级
修改
重置
返回
病毒扫描
认证后立即执行内存
启用全盘扫描
杀毒软件监视
全部监视
文件监视
脚本监视
处理方式
杀毒软件安装程序URL:
杀毒软件不合格时提示
杀毒引擎及病毒库升级

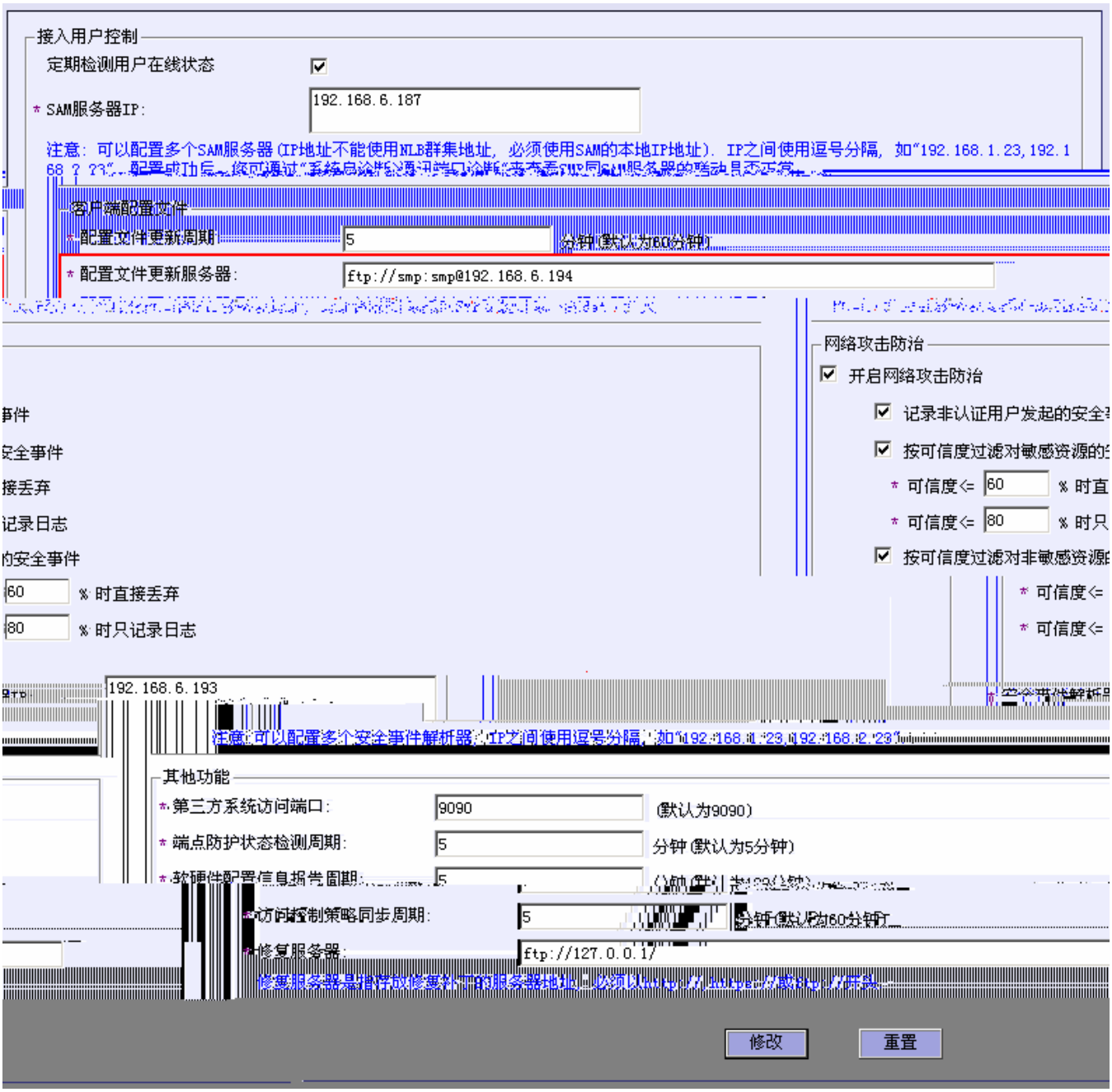
“ ”

1.3.3

”

“ ” “ ” “ ” FTP

ftp://[ ]:[ ]@[SMP IP]



“ ”

1.4

PC RG-SMP

1.4.1

1.1

1.4.2

“ > ” “ ”


微软补丁更新
启用微软补丁更新
更新服务器设置
更新服务器类型:
不指定更新服务器
锐捷客户端更新
启用锐捷客户端更
必须安装的补丁类型
全部类型
安全更新程序
关键更新程序
Feature Pack
Service Pack
周期:
16
http://support.microsoft.com/kb/927891/zh-cn
验证URL
WUA下载地址:
更新过程采取安全措施
如果采取安全措施，用户在
完成补丁更新之前，将按照端点防护处理方式进行处理(如下发警告消息、绑定端点防护模板等).
微软客户端更新控制
启用自动更新
允许自动更新立即安装:
配置自动更新:
启用
自动下载并计划安装
计划安装时间:
10:00
返回
添加
重置
注意：重置功能将重置所有选项卡中的信息。

“ ”

1.4.3

1.3.4

1.4.4

1.3.5

1.5

RG-SMP PC / / /

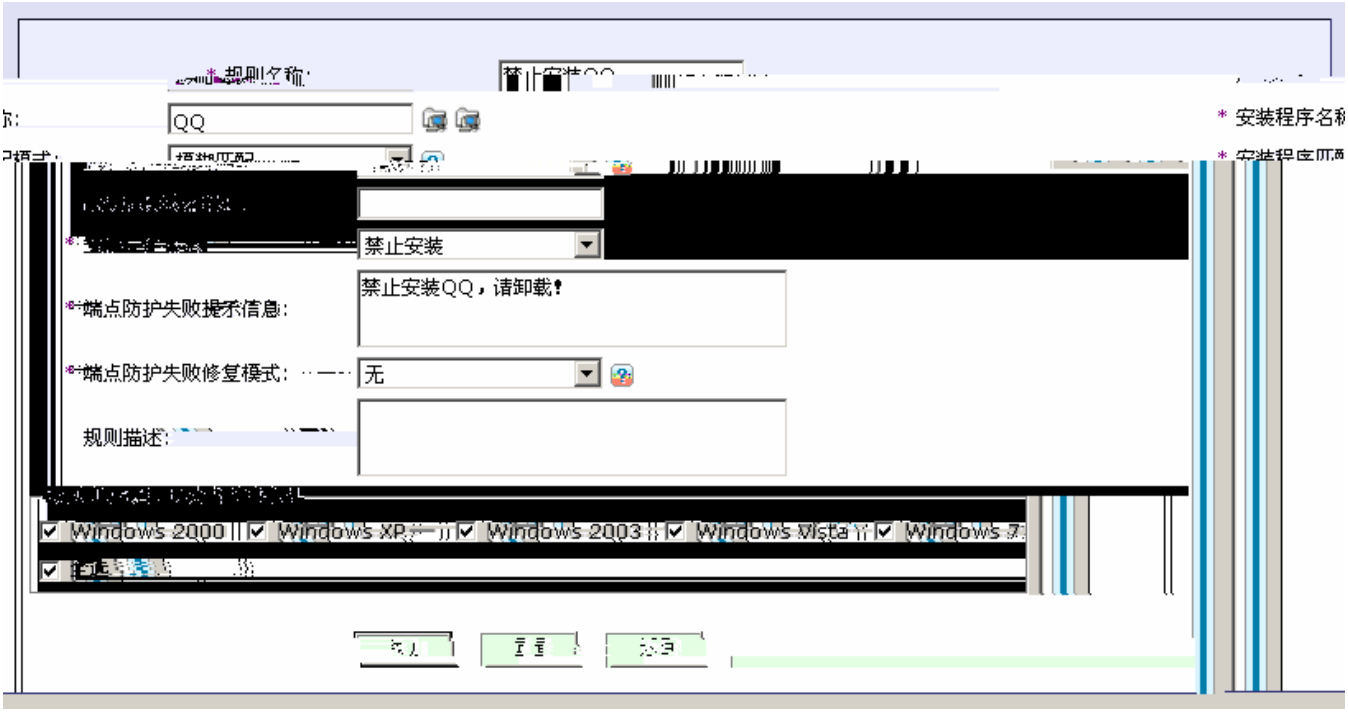
1.5.1

1.1

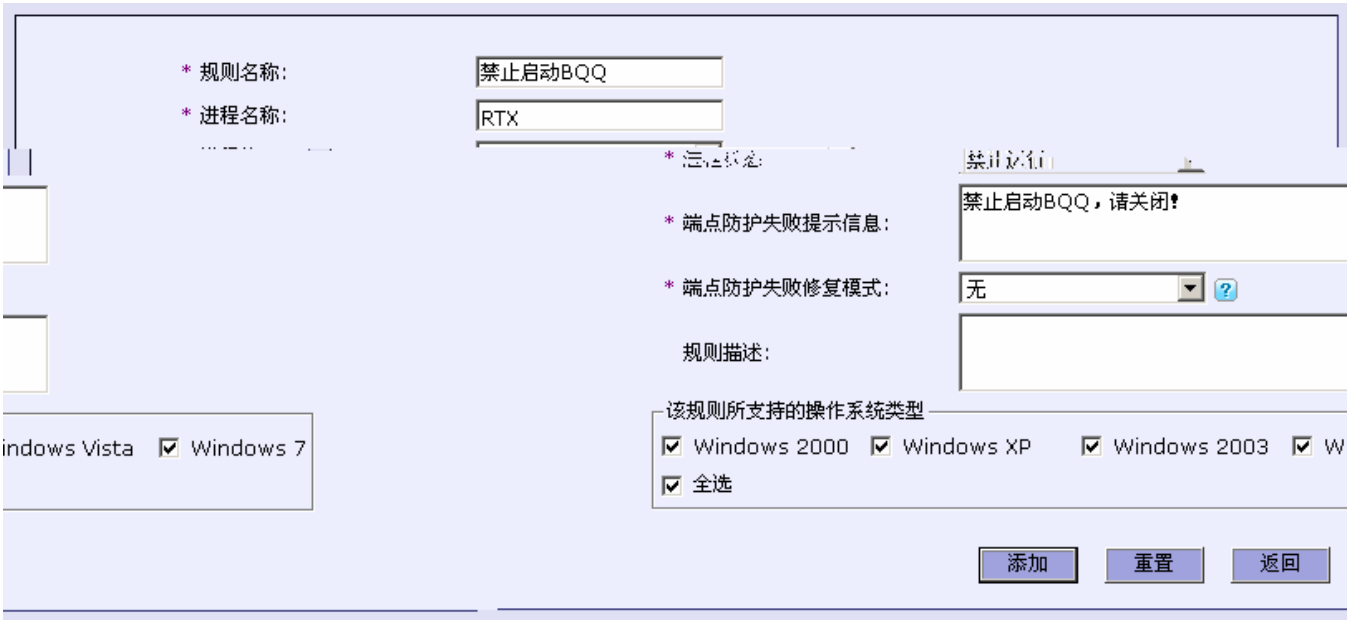
1.5.2

“ ” “ ”

“ ”



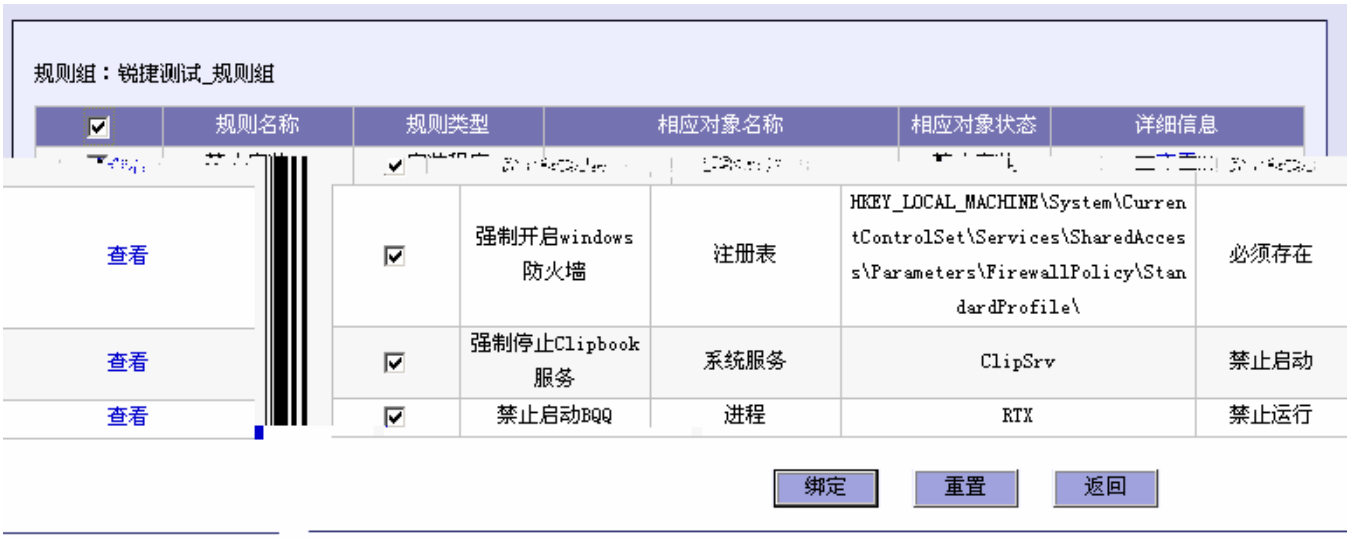
“ ”


* 规则名称:
禁止启动BQQ
* 进程名称:
RTX
* 端点防护失败提示信息:
禁止启动BQQ，请关闭!
* 端点防护失败修复模式:
无
规则描述:
该规则所支持的操作系统类型
Windows 2000
Windows XP
Windows 2003
全选
添加
重置
返回

“ ”


* 规则名称:
强制开启windows防火墙
* 注册表分支名称:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\
启动项快捷方式
* 注册表键名:
EnableFirewall
注册表键值类型:
REG_DWORD
键值表达式:
等于
* 注册表键值:
1
* 注册表状态:
必须存在
* 端点防护失败提示信息:
系统检测到您的计算机已经关闭windows防
* 端点防护失败修复模式:
强制修复
规则描述:
该规则所支持的操作系统类型
Windows 2000
Windows XP
Windows 2003
Windows Vista
全选
注意：如果选择“强制修复”模式，当注册表状态为“必须存在”时，将对注册表键值进行修复；当注
为“禁止存在”，将删除注册表键值。
修改
重置
返回

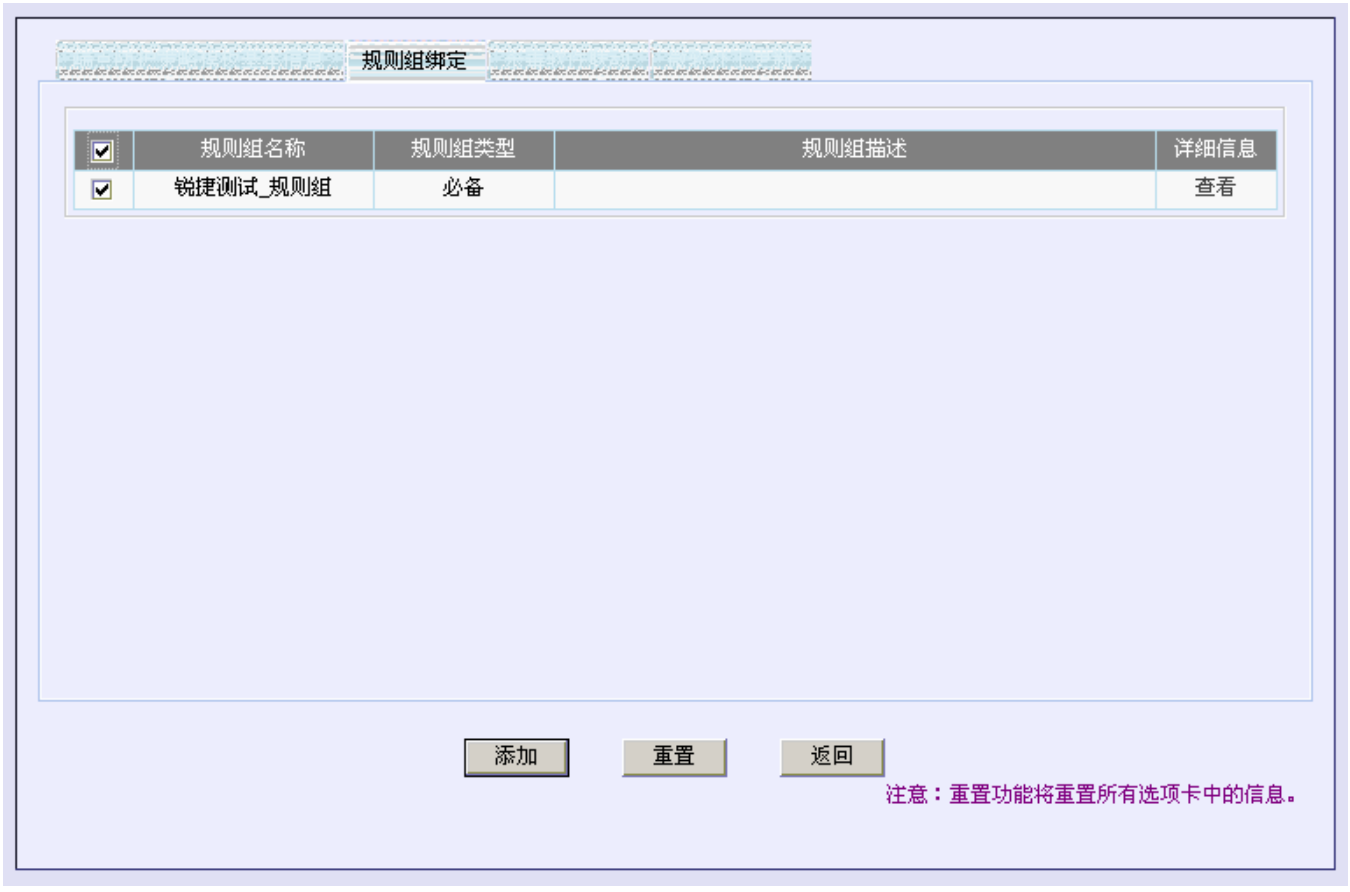
“ ”


规则组：锐捷测试_规则组
规则名称
规则类型
相应对象名称
相应对象状态
详细信息
查看
强制开启windows防火墙
注册表
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\
必须存在
查看
强制停止Clipbook服务
系统服务
ClipSrv
禁止启动
查看
禁止启动BQQ
进程
RTX
禁止运行
绑定
重置
返回

“ ”

1.5.4

“ ” “ ”


规则组绑定
规则组名称
规则组类型
规则组描述
详细信息
锐捷测试_规则组
必备
查看
添加
重置
返回
注意：重置功能将重置所有选项卡中的信息。

“ ”

1.5.5

1.3.4

1.5.6

1.3.5

1.6

RG-SMP PC
RG-SMP PCMCIA
U

1.6.1

1.1

1.6.2

“ ›

“ ”

1.6.3

1.3.5

1.7

RG-SMP PC

RG-Supplicant PC

RG-Supplicant

RG-Supplicant

1.7.1

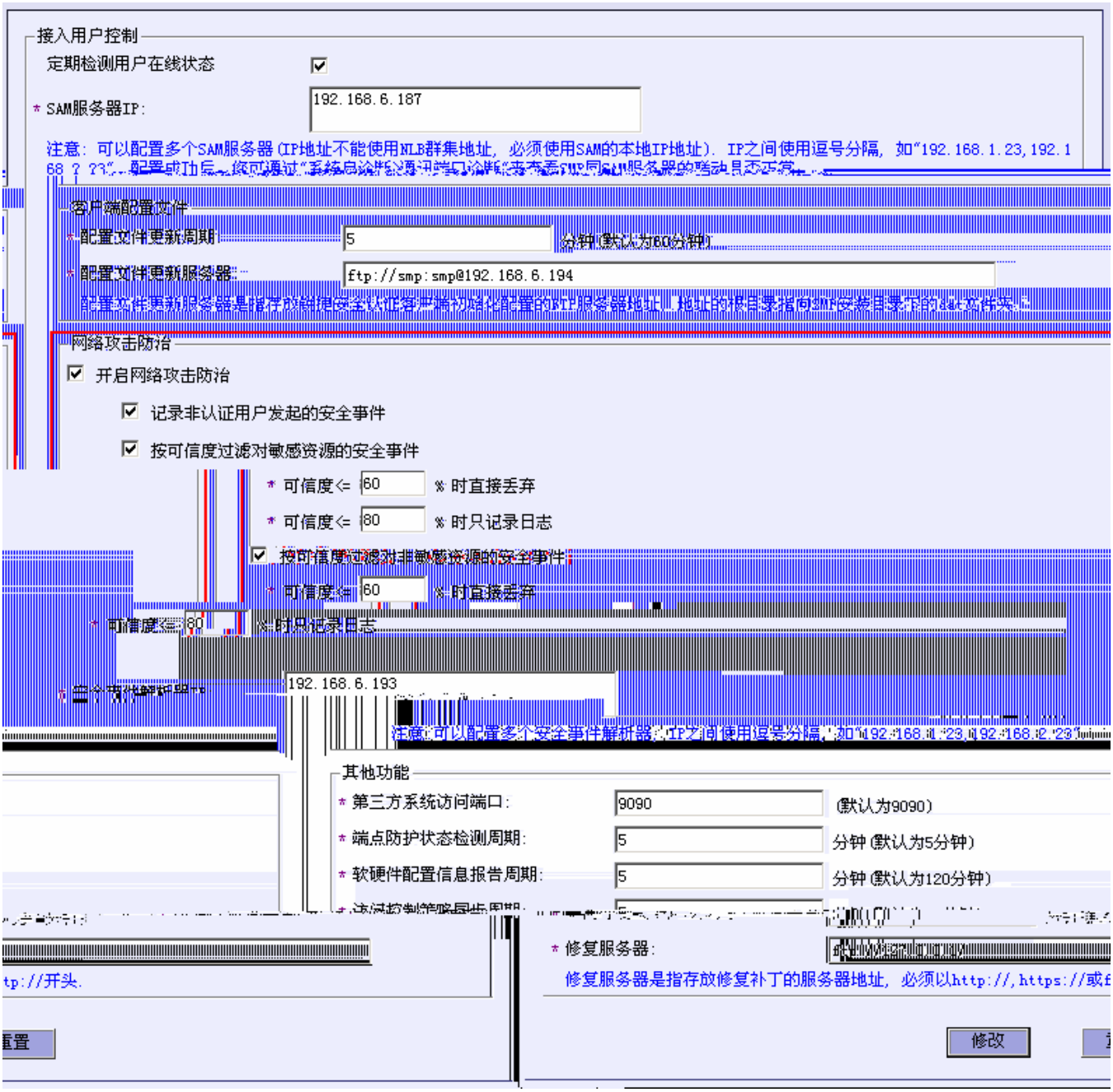
1.1

1.7.2

“ ” “ ”

1.8.2 RG-SEP

“ ” “ ” RG-SEP

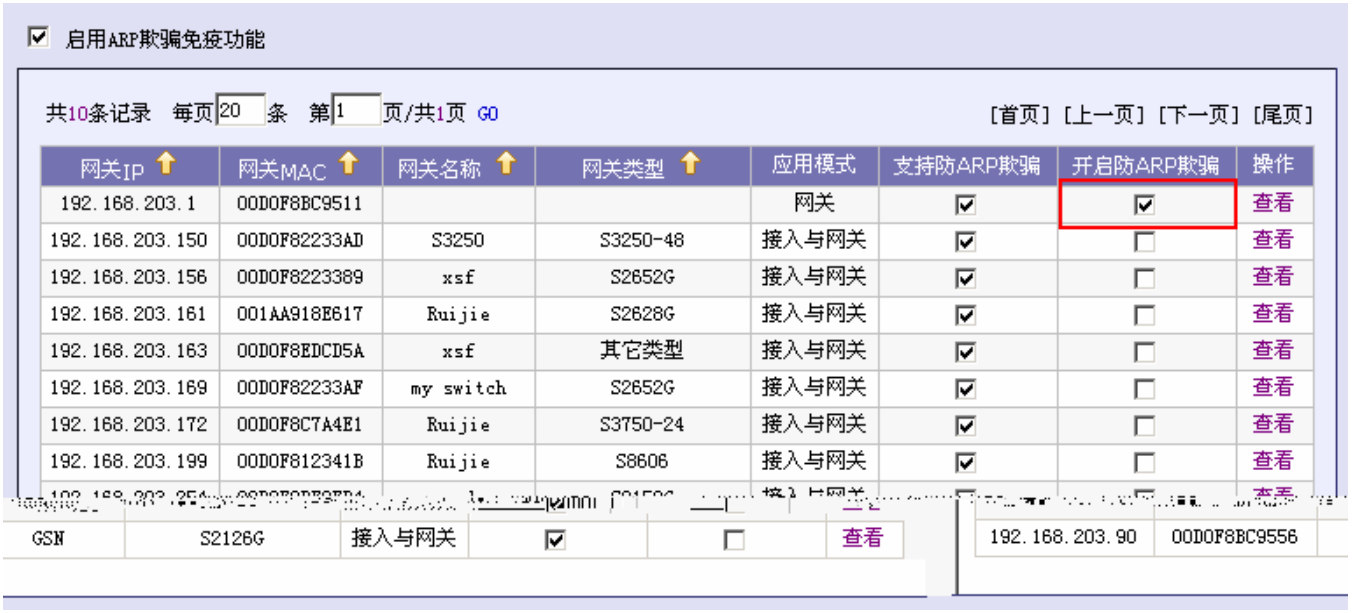


“ ”

1.8.3

“

“ ARP ”



说明

、 “ ARP ” ARP

、 “ ARP ” ARP ARP

2

Red-Giant Security Management Platform SMP)

SMP

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

2.1

SMP

- ____
- _____
- _____
- _____
- _____

2.1.1

SMP

Õ ----- SMP supervisor ruijiesmp

Õ ----- SMP log 111111111

Õ ----- SMP SMP admin 111111111

2.1.2

SMP

Õ supervisor ruijiesmp

Õ log 111111111

Õ admin 111111111

注意

2.1.3

“ ” “ ”

“ ”

“ ”

“ ”

2.1.4

“ ”

2.1.5

supervisor

2.1.5.1

“ ” “ ”


用户名:
创建时间 (开始):
所属用户组:
所有用户组
创建时间 (结束):
查询
重置
添加
删除所选
共3条记录 每页20 条 第1 页/共1页 GO
[首页] [上一页] [下一页] [尾页]
用户名
所属用户组
创建时间
操作
admin
系统管理员
2009-07-17 11:29:53
查看 修改
log
日志管理员
2009-07-17 11:29:53
查看 修改
supervisor
超级管理员
2009-07-17 11:29:53
查看 修改

“ ” “ ” “ ”

“ ” “ ”

ü “ ” “ ” “ ”

ü “ ” “ ”

ü

ü “ ” “ ” “ ”

说明

2.1.5.2

“ ” “ ” “ ”

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

’

“*”

’

SUPERVISOR( ) system( ) 9

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

，

， 9 20

， supervisor

2.1.5.4

“ ” “ ”

2.2

SMP

，

，

，

- [_____]
- [_____]
- [_____]
- [_____]

2.2.1

Õ , RG-SAM
, ,

Õ

Õ

1 2 1

Õ

1 2 1

2.2.2

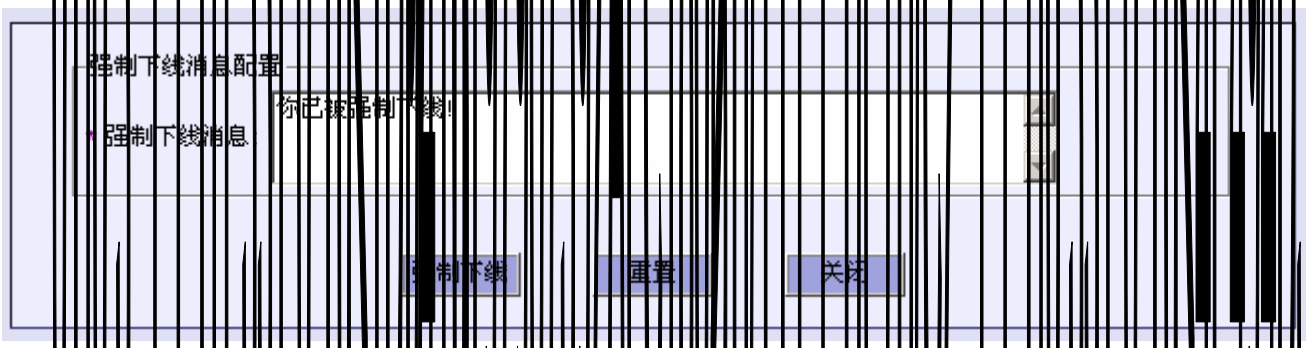
SMP
SMP SAM

2.2.2.1

“ ” “ ” “ ”

2.2.2.3

“ ” “ ” “ ”



“ ” SMP

“ ”

“ ”

说明

“ ”

2.2.2.4

“ ” “ ”

说明

说明

，

，

2.2.2.6

“ ” “ ” “ ”

“ ”

“

“

“

URL URL

“ ”

2.2.3

SMP

2.2.3.1

“ ” “ ” “ ”

“ ” “ ” “ ”

“ ” “ ”

ü “ ” “ ” “ ”

ü “ ” “ ”

ü

ü

ü “ ” “ ” “ ”

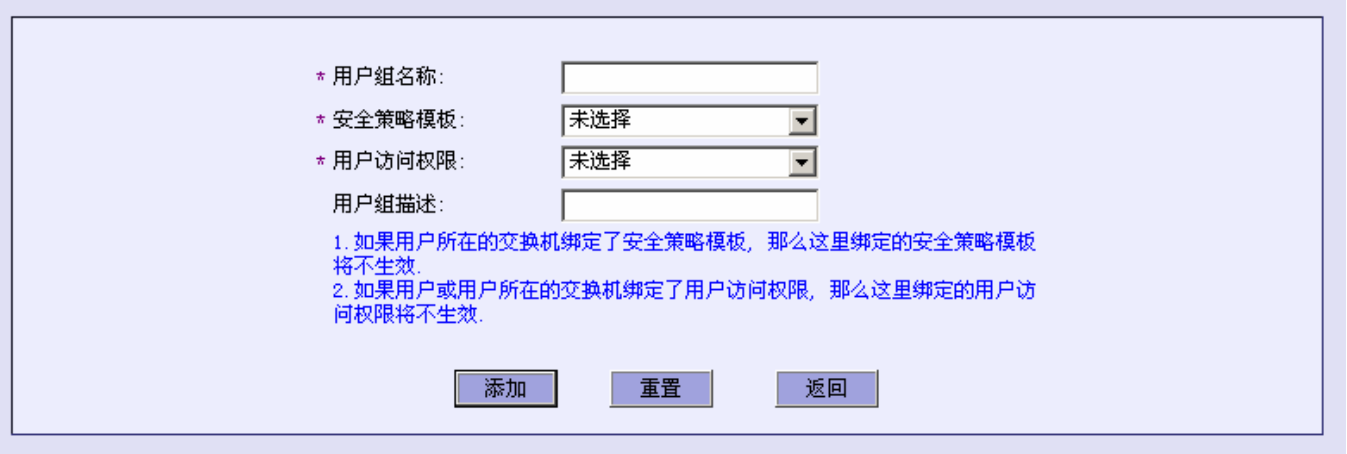
”

说明

，

2.2.3.2

“ ” “ ” “ ”



“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

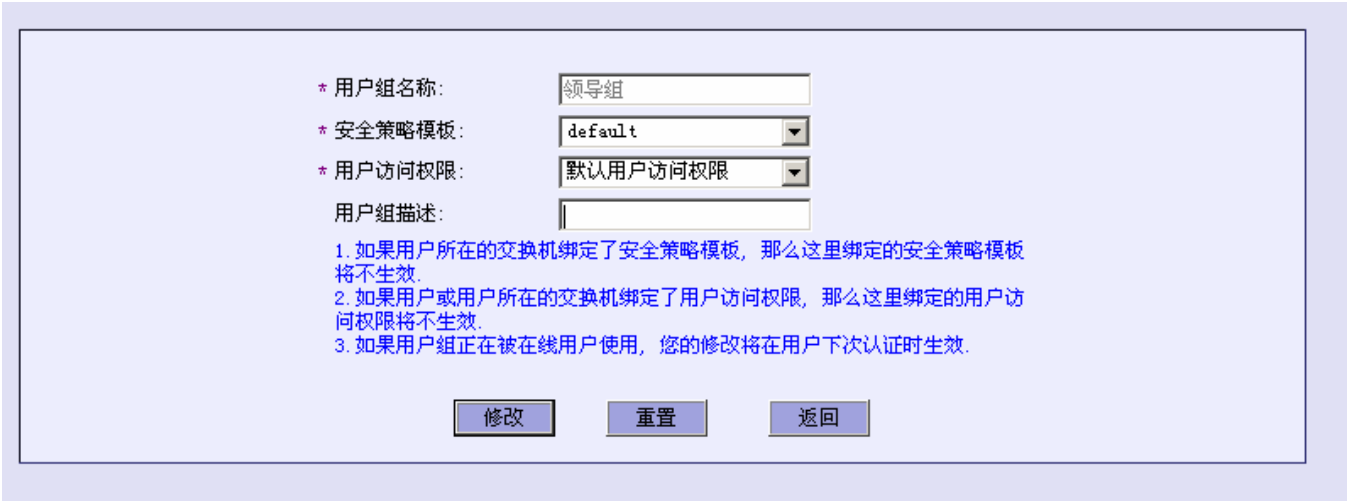
说明

，“*” 32 16

，

2.2.3.3

“ ” “ ” “ ”



“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

，

，

2.2.3.4

“ ” “ ”

说明

，

2.2.4

SMP

2.2.4.1

“ ” “ ” “ ”

“ ” “ ” “

”

“ ” “ ”

ü “ ” “ ” “

”

ü “ ” “

”

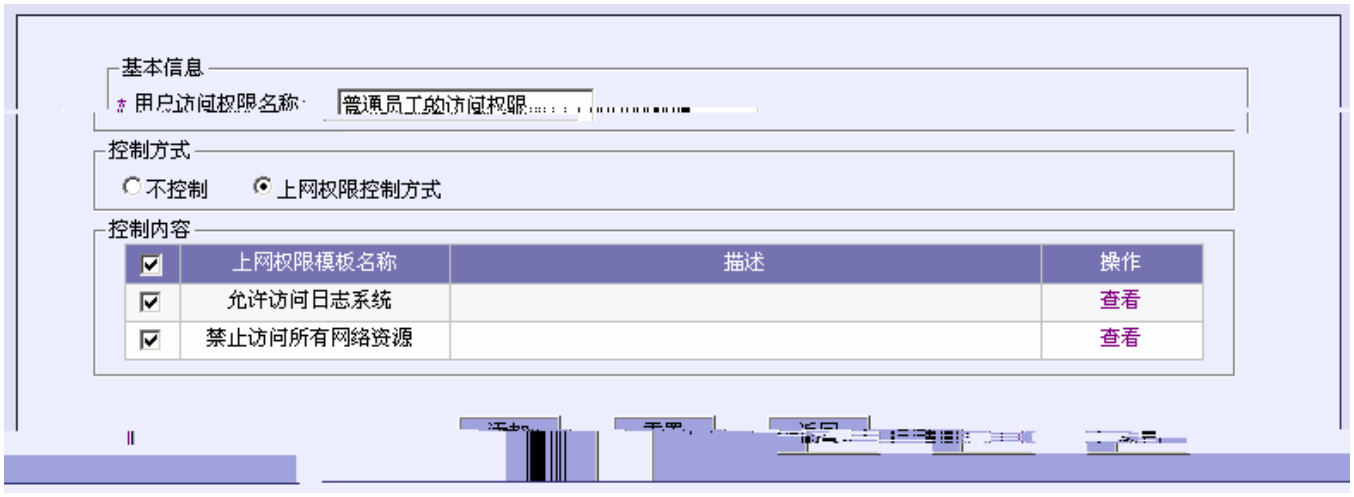
ü

ü “ ” “ ” “

”

2.2.4.2

“ ” “ ” “ ”


基本信息
用户访问权限名称：
普通员工的访问权限
控制方式
不控制
上网权限控制方式
控制内容
上网权限模板名称
描述
操作
允许访问日志系统
查看
禁止访问所有网络资源
查看

“ ”

“ ” “ ” “ ”

“ ”

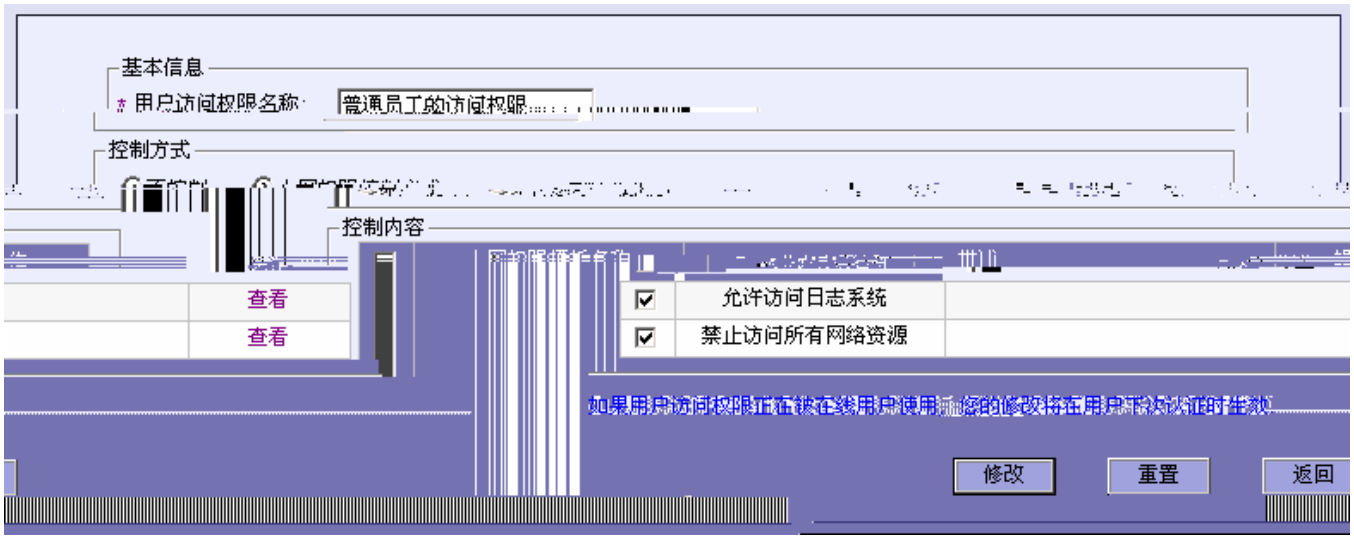
“ ” “ ”

说明

- “*” 32 16
- “ ”
- “ ”
- “ ”

2.2.4.3

“ ” “ ” “ ”


基本信息
用户访问权限名称
普通员工的访问权限
控制方式
控制内容
查看
查看
允许访问日志系统
禁止访问所有网络资源
修改
重置
返回

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

，

，

2.2.4.4

“ ” “ ”

说明

，

，

2.2.5

SMP

2.2.5.1

“ ” “ ” “ ”

“ ” “ ” “

”

“ ” “ ”

“ ”

ü “ ” “ ” “

”

ü “ ” “

”

ü

ü “ ” “ ”

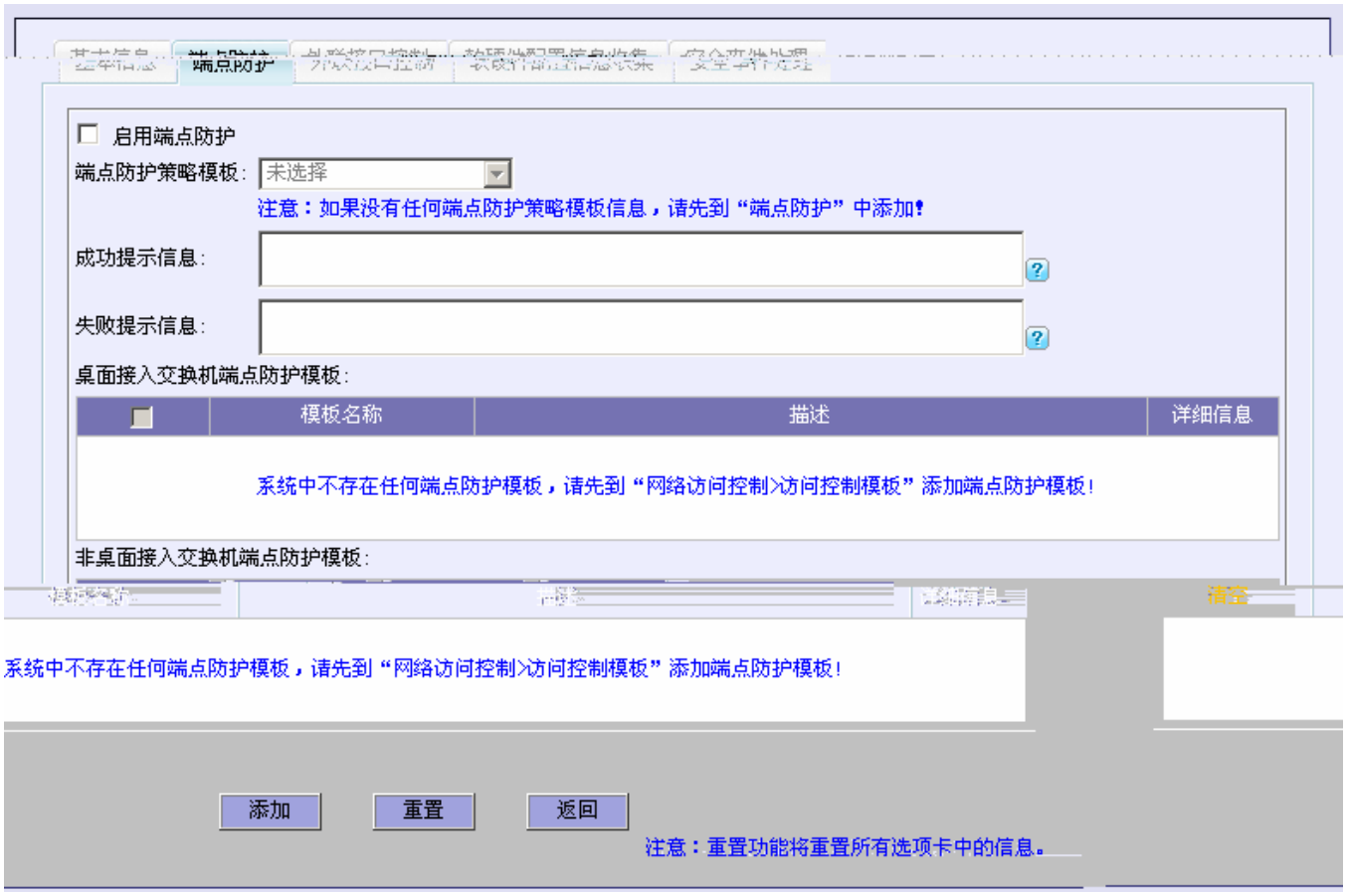
“ ”

2.2.5.2

“ ” “ ” “ ”


* 安全策略模板名称:
安全策略模板描述:
* 安全策略模板具体信息请查看各标签卡项
添加
重置
返回
注意：重置功能将重置所有选项卡中的信息。

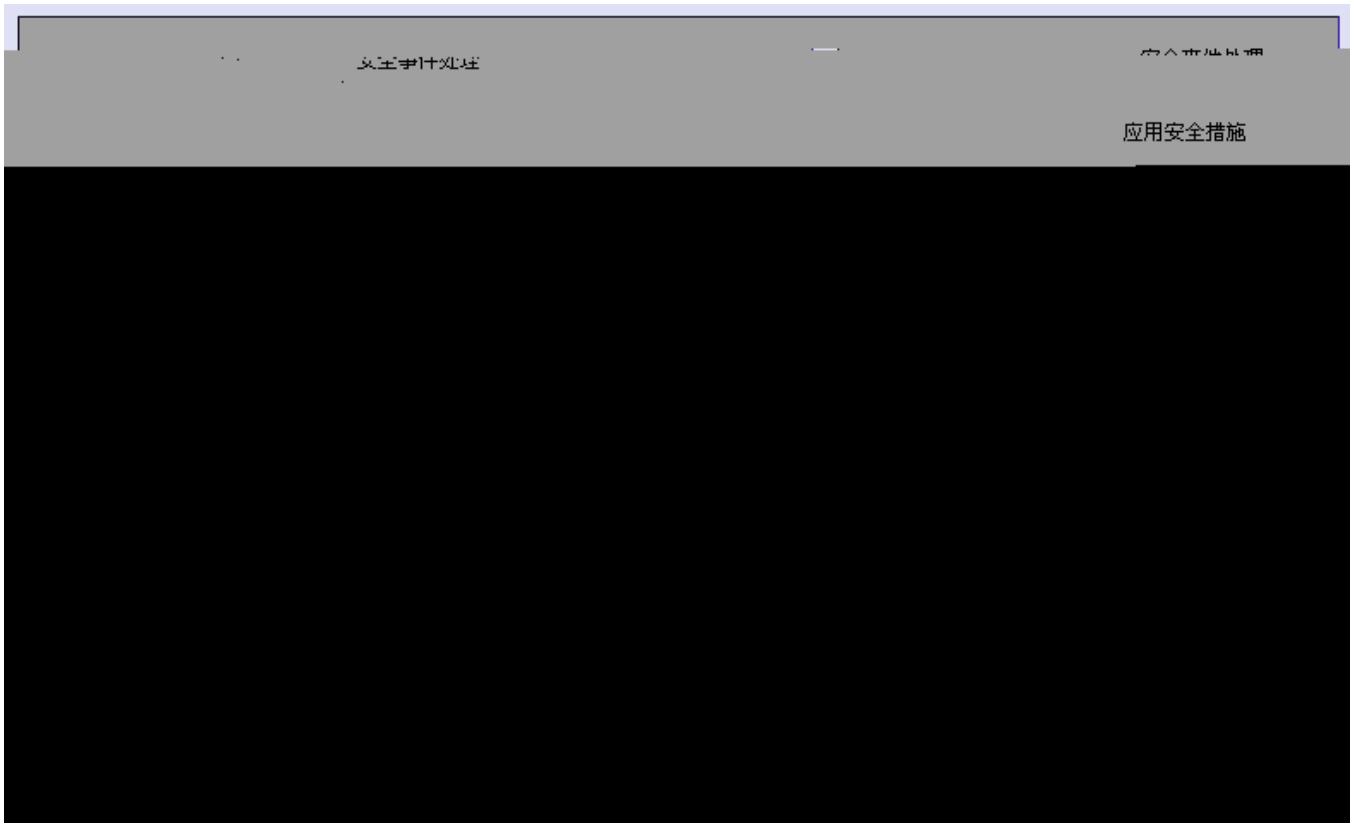
“ ”


端点防护
启用端点防护
端点防护策略模板:
未选择
注意：如果没有任何端点防护策略模板信息，请先到“端点防护”中添加!
成功提示信息:
失败提示信息:
桌面接入交换机端点防护模板:
模板名称
描述
详细信息
系统中不存在任何端点防护模板，请先到“网络访问控制>访问控制模板”添加端点防护模板!
非桌面接入交换机端点防护模板:
系统中不存在任何端点防护模板，请先到“网络访问控制>访问控制模板”添加端点防护模板!
添加
重置
返回
注意：重置功能将重置所有选项卡中的信息。

“ ”


外联接口控制
外联接口名称
控制方式
提示信息
PCMCIA接口
不进行控制
串口
不进行控制
智能卡读卡器
不进行控制
红外线接口
不进行控制
打印机
不进行控制
磁带机
不进行控制
软盘驱动器
不进行控制
光盘驱动器
不进行控制
U盘
不进行控制
添加
重置
返回
注意：重置功能将重置所有选项卡中的信息。

“ ”



“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

“*” 32 16

“ ”

“ ”

”

，

2.2.5.3

“ ” “ ” “ ”


基本信息
端点防护
外联接口控制
软硬件配置信息收集
安全事件处理
default
* 安全策略模板名称
各标签卡项
* 安全策略模板具体信息请查看
修改
重置
返回

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

，

，

“ ”

“ ” “ ”

›

2.2.5.4

“ ” “ ”

说明

›

2.3

SMP

- ›
- ›
- ›
- ›
- ›

2.3.1

Õ

“ 2008 ”

Õ

Õ

Õ

Õ

Õ

2.3.2

SMP

2.3.2.1

“ ” “ ” “

”

“ ” “ ” “

”

“ ” “ ”

ü “ ” “ ”

“ ”

ü “ ” “

”

ü

ü “ ” “ ”

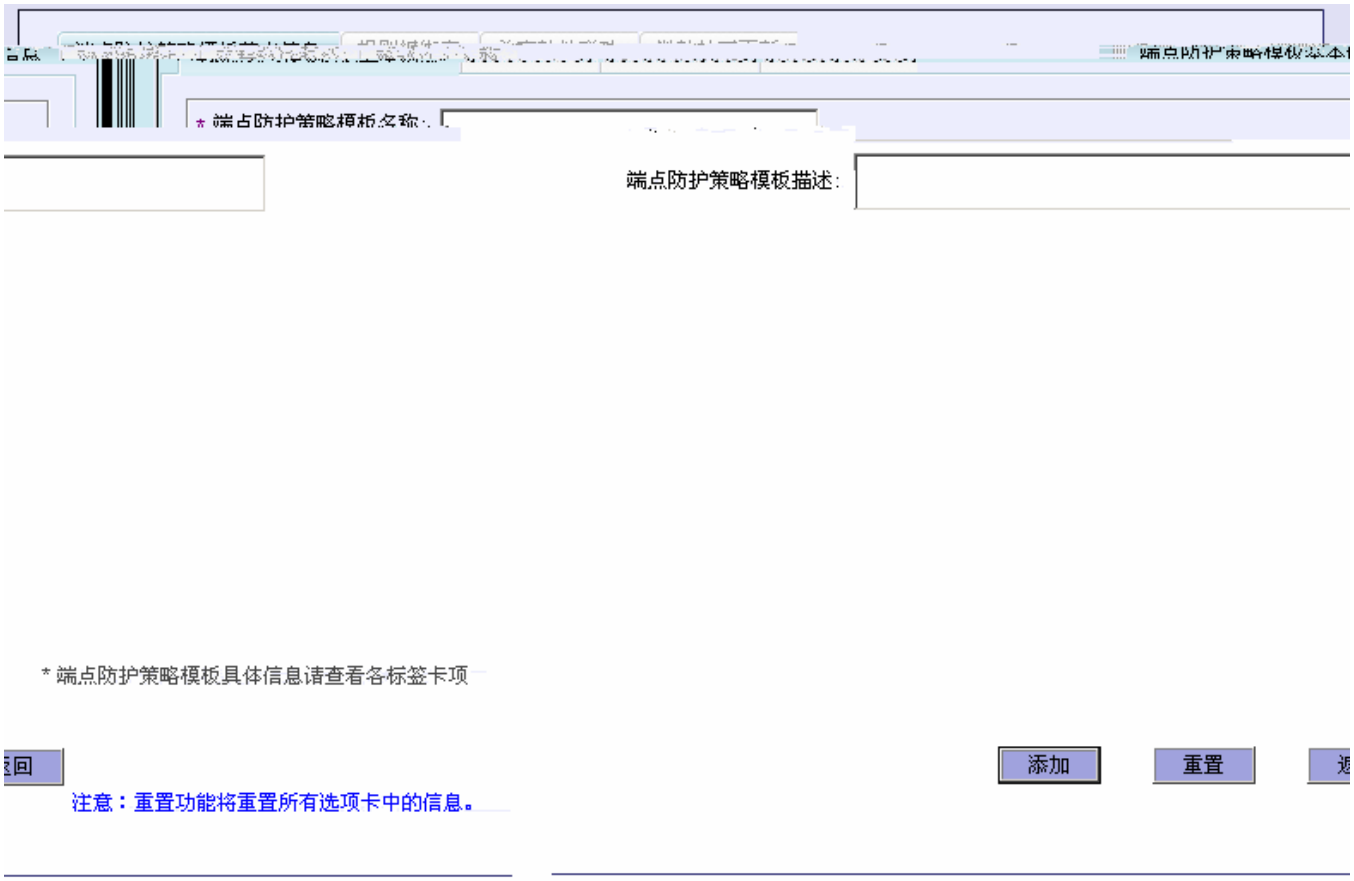
“ ”

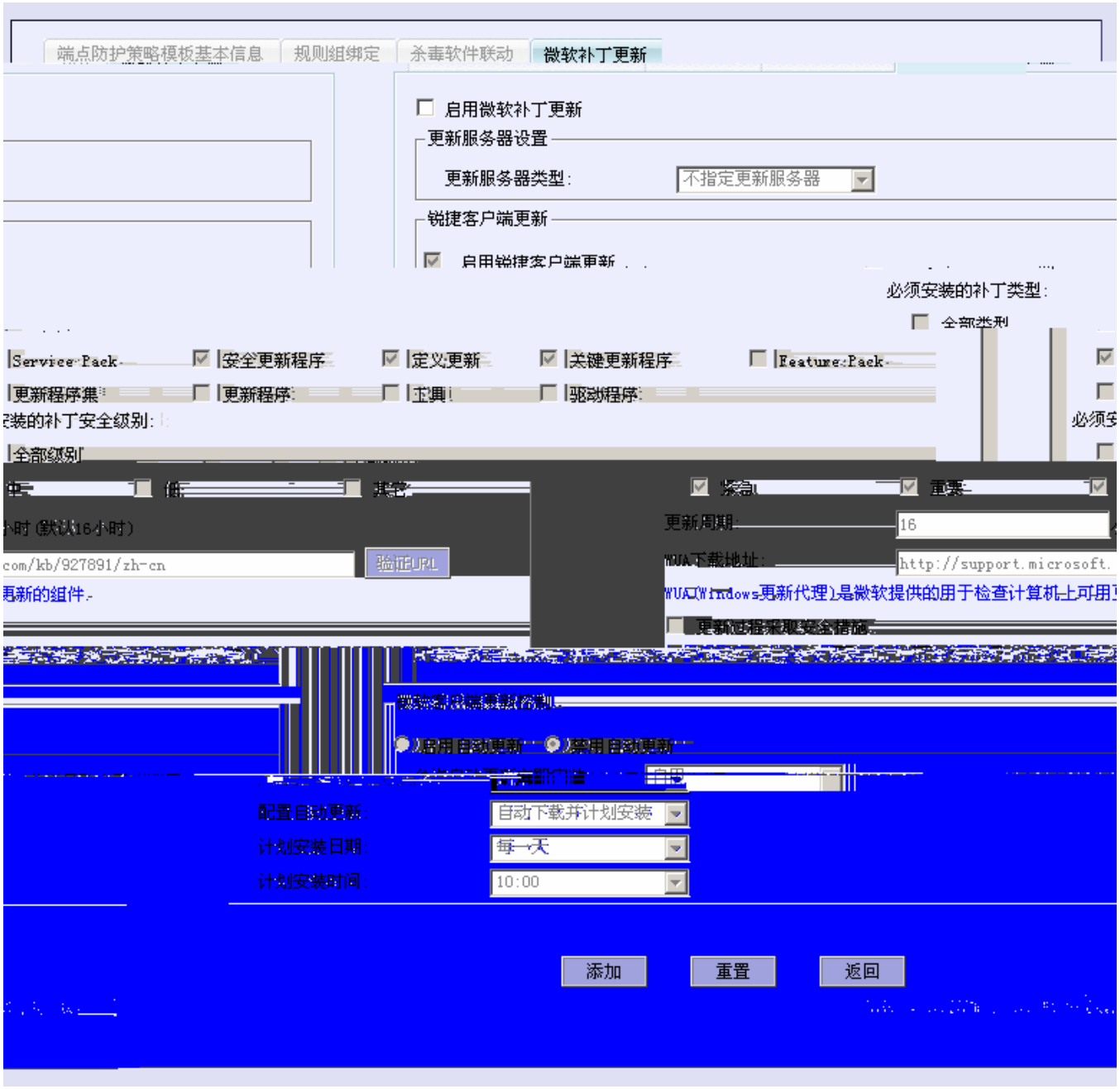
说明

，

2.3.2.2

“ ” “ ” “ ”


端点防护策略模板描述:
* 端点防护策略模板具体信息请查看各标签卡项
添加
重置
注意：重置功能将重置所有选项卡中的信息。


端点防护策略模板基本信息
规则组绑定
杀毒软件联动
微软补丁更新
启用微软补丁更新
更新服务器设置
更新服务器类型:
不指定更新服务器
锐捷客户端更新
必须安装的补丁类型:
Service Pack
安全更新程序
定义更新
关键更新程序
Feature Pack
更新程序集
更新程序
驱动程序
全部级别
更新周期:
16
验证URL
http://support.microsoft.
配置自动更新:
自动下载并计划安装
计划安装日期:
每一天
计划安装时间:
10:00
添加
重置
返回

“ ”

“ ” “ ” “

”

“ ”

“ ” “ ”

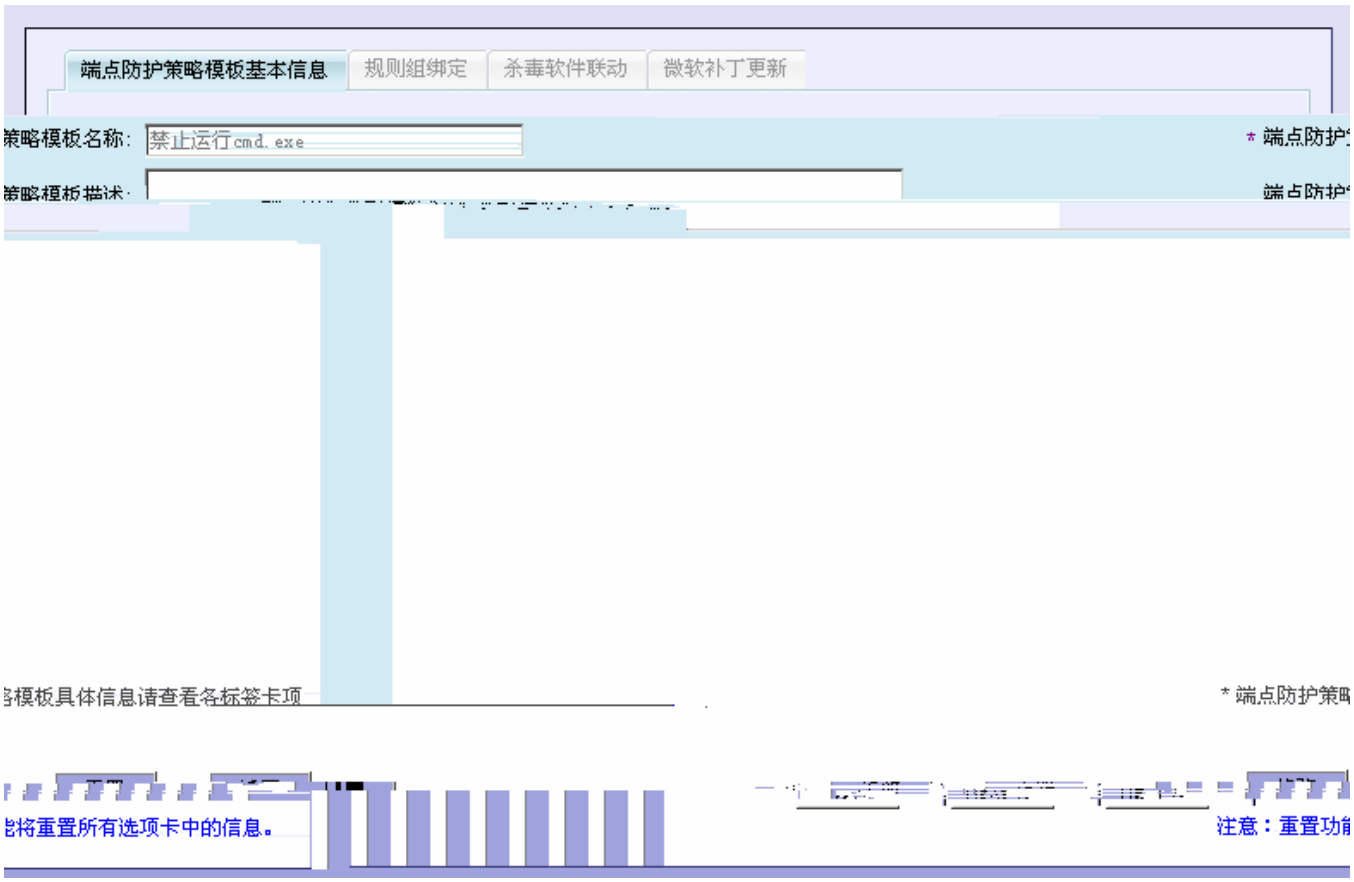
说明

“*” 32 16

2.3.2.3

“ ” “ ” “

”


端点防护策略模板基本信息
规则组绑定
杀毒软件联动
微软补丁更新
策略模板名称:
禁止运行cmd.exe
* 端点防护
模板具体信息请查看各标签卡项
* 端点防护策略
将重置所有选项卡中的信息。
注意：重置功能

“ ”

“ ” “ ” “

”

“ ”

“ ” “ ”

说明

，

，

2.3.2.4

“ ” “ ”

说明

，

2.3.2.5

说明

“ ”

，

，

“ ”

，

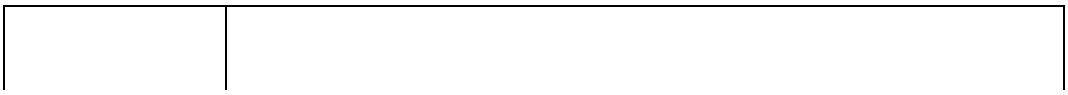
( )

， WUA(Windows) WUA

，

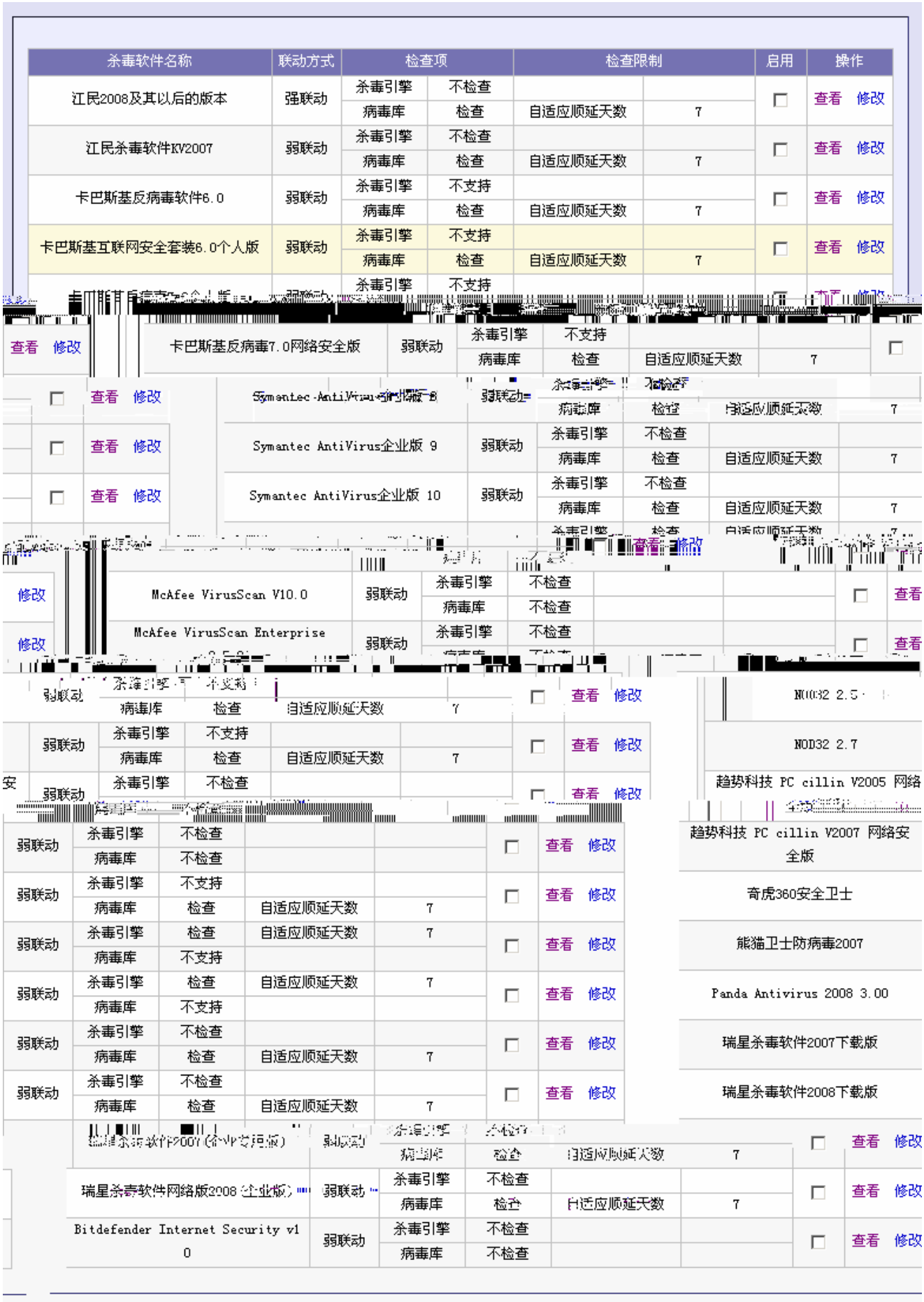
， Windows

，



2.3.3.1

“ ” “ ” “ ”



杀毒软件名称	联动方式	检查项		检查限制		启用	操作
江民2008及其以后的版本	强联动	杀毒引擎	不检查				查看 修改
		病毒库	检查	自适应顺延天数	7		
江民杀毒软件KV2007	弱联动	杀毒引擎	不检查				查看 修改
		病毒库	检查	自适应顺延天数	7		
卡巴斯基反病毒软件6.0	弱联动	杀毒引擎	不支持				查看 修改
		病毒库	检查	自适应顺延天数	7		
卡巴斯基互联网安全套装6.0个人版	弱联动	杀毒引擎	不支持				查看 修改
		病毒库	检查	自适应顺延天数	7		
		杀毒引擎	不支持				
查看 修改	卡巴斯基反病毒7.0网络安全版	弱联动	杀毒引擎	不支持			
			病毒库	检查	自适应顺延天数	7	
查看 修改	Symantec AntiVirus [illegible]	弱联动	[illegible]				
			病毒库	检查	自适应顺延天数	7	
查看 修改	Symantec AntiVirus企业版 9	弱联动	杀毒引擎	不检查			
			病毒库	检查	自适应顺延天数	7	
查看 修改	Symantec AntiVirus企业版 10	弱联动	杀毒引擎	不检查			
			病毒库	检查	自适应顺延天数	7	
			[illegible]				
修改	McAfee VirusScan V10.0	弱联动	杀毒引擎	不检查			查看
			病毒库	不检查			
修改	McAfee VirusScan Enterprise	弱联动	杀毒引擎	不检查			查看
			[illegible]				
	弱联动	杀毒引擎	不支持				查看 修改
		病毒库	检查	自适应顺延天数	7		
	弱联动	杀毒引擎	不支持				查看 修改
		病毒库	检查	自适应顺延天数	7		
安	弱联动	杀毒引擎	不检查				查看 修改
		病毒库	不检查				
弱联动	杀毒引擎	不检查				查看 修改	
	病毒库	不检查					
弱联动	杀毒引擎	不支持				查看 修改	
	病毒库	检查	自适应顺延天数	7			
弱联动	杀毒引擎	检查	自适应顺延天数	7		查看 修改	
	病毒库	不支持					
弱联动	杀毒引擎	检查	自适应顺延天数	7		查看 修改	
	病毒库	不支持					
弱联动	杀毒引擎	不检查				查看 修改	
	病毒库	检查	自适应顺延天数	7			
弱联动	杀毒引擎	不检查				查看 修改	
	病毒库	检查	自适应顺延天数	7			
[illegible]	弱联动	[illegible]				查看 修改	
		病毒库	检查	自适应顺延天数	7		
瑞星杀毒软件网络版2008（企业版）	弱联动	杀毒引擎	不检查			查看 修改	
		病毒库	检查	自适应顺延天数	7		
Bitdefender Internet Security v1 0	弱联动	杀毒引擎	不检查			查看 修改	
		病毒库	不检查				

NOD32 2.5

NOD32 2.7

趋势科技 PC cillin V2005 网络

趋势科技 PC cillin V2007 网络安全版

奇虎360安全卫士

熊猫卫士防病毒2007

Panda Antivirus 2008 3.00

瑞星杀毒软件2007下载版

瑞星杀毒软件2008下载版

ü “ ” “ ” “ ”

2.3.3.2

“ ” “ ” “ ”

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

,

“ ” “

,

”

“ ”

2.3.4

SMP

2.3.4.1

“ ” “ ” “ ” “ ”

“ ”

“ ” “ ” “ ”

“ ” “ ”

ü “ ” “ ” “ ”

ü “ ” “ ”

ü

ü “ ” “ ” “ ”

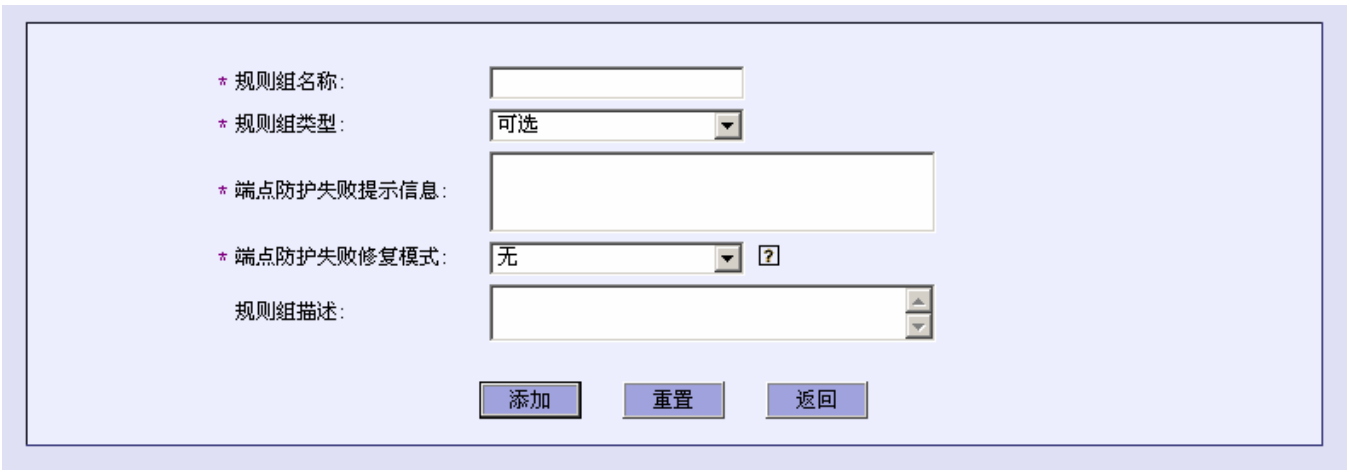
ü “ ” “ ” “ ”

说明

›

2.3.4.2

“ ” “ ” “ ”


* 规则组名称:
* 规则组类型:
可选
* 端点防护失败提示信息:
* 端点防护失败修复模式:
无
规则组描述:
添加
重置
返回

“ ”

“ ” “ ”

“ ” “ ” “ ”


规则组：fewafewfwa
规则名称
规则类型
相应对象名称
相应对象状态
详细信息
禁止运行cmd. exe
进程
cmd. exe
禁止运行
查看
绑定
重置
返回

“ ” “ ”

“ ” “ ”

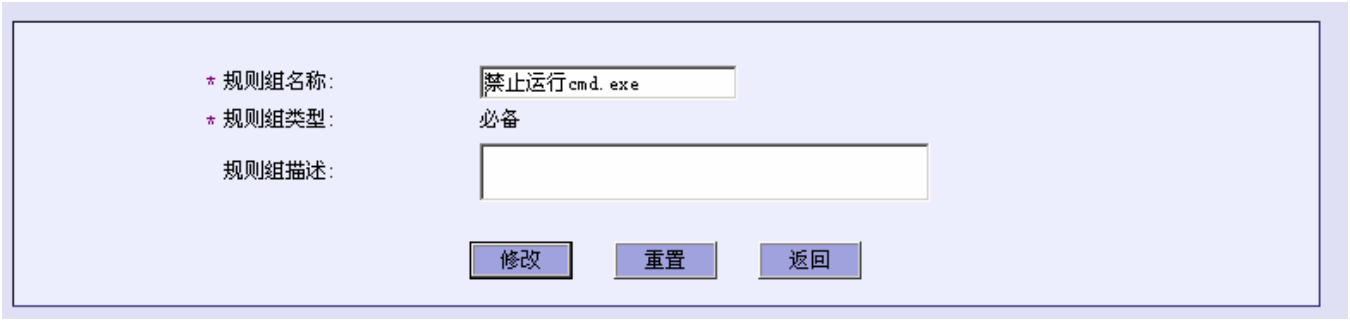
“ ” “ ” “ ”

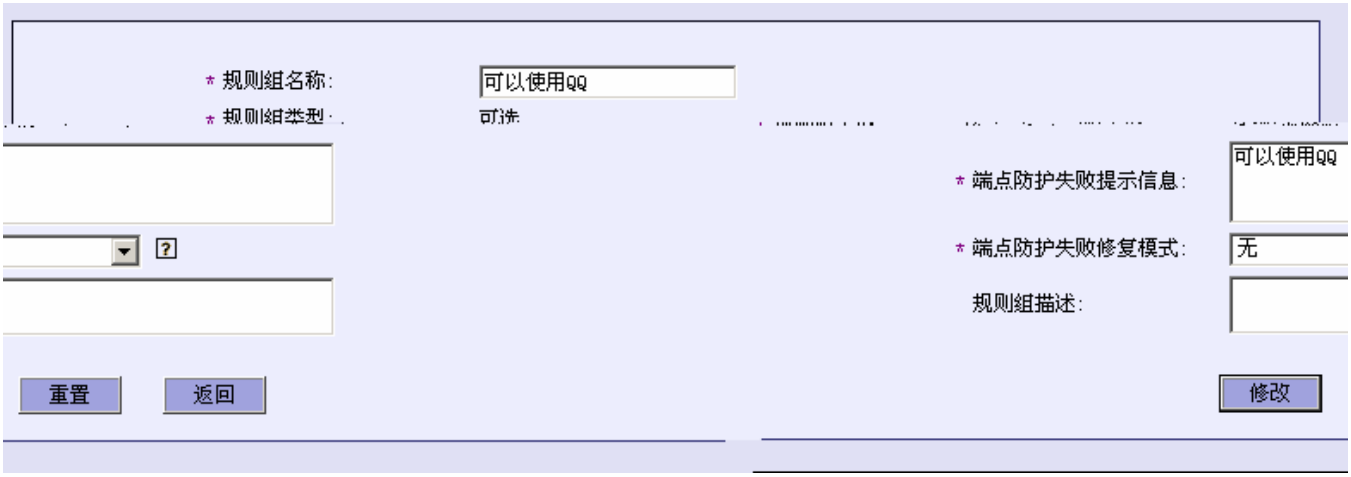
说明

- “*” 64 32
- “ ” “ ” “ ”
- “ ”

2.3.4.3

“ ” “ ” “ ”


* 规则组名称:
禁止运行cmd.exe
* 规则组类型:
必备
规则组描述:
修改
重置
返回


* 规则组名称:
可以使用QQ
* 端点防护失败提示信息:
可以使用QQ
* 端点防护失败修复模式:
无
规则组描述:
重置
返回
修改

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

> **说明**
>
> 。

2.3.4.4

“ ” “ ”

说明

，

2.3.4.5

“ ” “ ” “ ”

“ ”

“ ” “ ” “ ”

“ ”

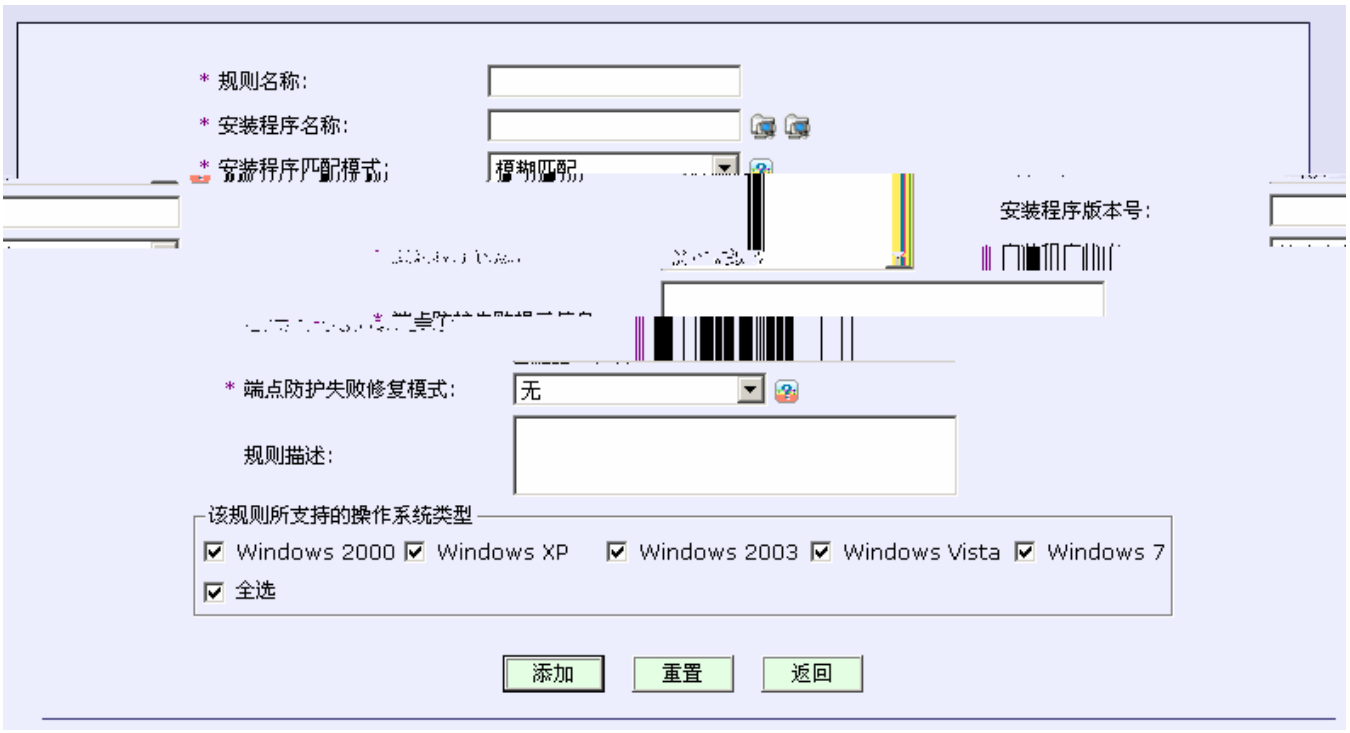
“ ” “ ”

2.3.5

SMP

2.3.5.1

“ ” “ ” “ ” “ ” “ ”



“ ”

“ ” “ ” “ ”

“ ”

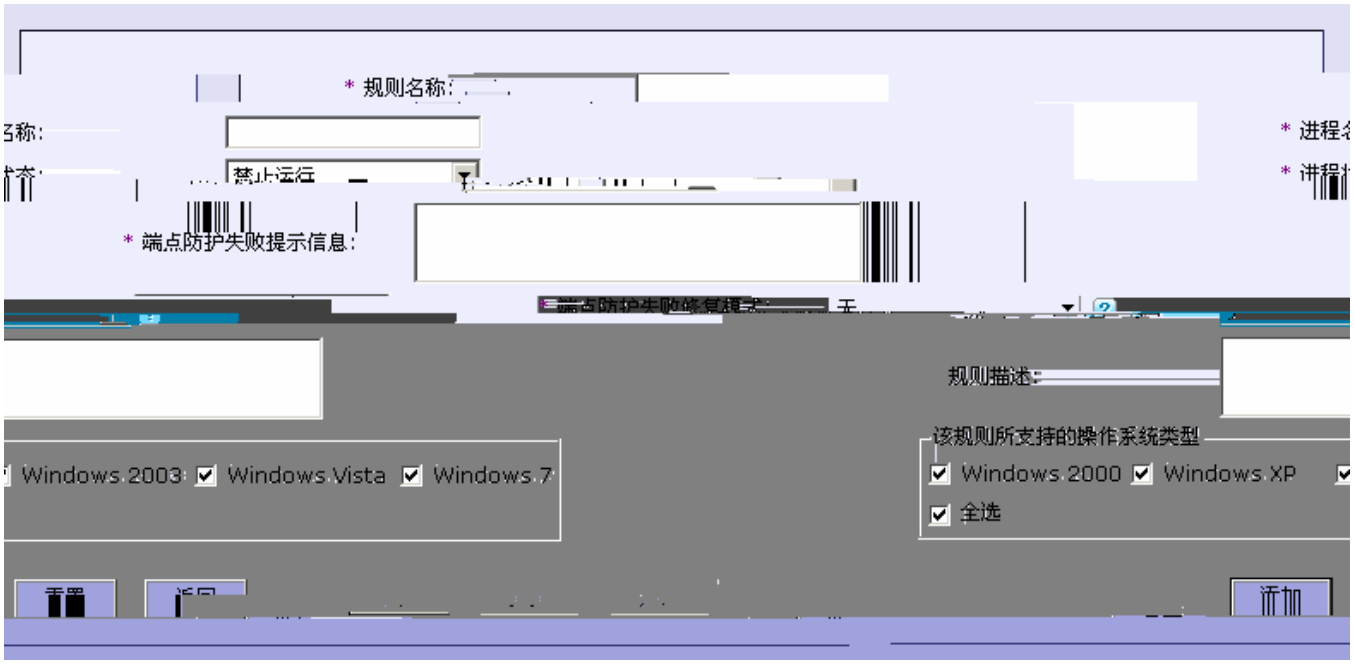
“ ” “ ”

说明

- “*” 128 64
-
- “ ” “ ” “ ”
  “ ”
-

2.3.5.3

“ ” “ ” “ ”



“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

“*” 128 64

2.3.5.4


* 规则名称:
* 注册表分支名称:
启动项快捷方式
注册表键名:
小于
禁止存在
无
Windows 2000
Windows XP
Windows 2003
Windows Vista
全选
添加
重置
返回

“ ”

“ ” “ ”

“ ”

“ ” “ ”

说明

“*” 128 64

“ ”

“

”

“ ”

›

2.3.5.5

“ ” “ ” “ ”

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

› “*” 128 64

›

›

›

2.3.5.6

“ ” “ ” “ ”

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

。

2.3.5.7

“ ” “ ”

说明

。

2.3.5.8

“ ” “ ” “ ” “ ” “ ”

“ …”

“ ”

“ ”

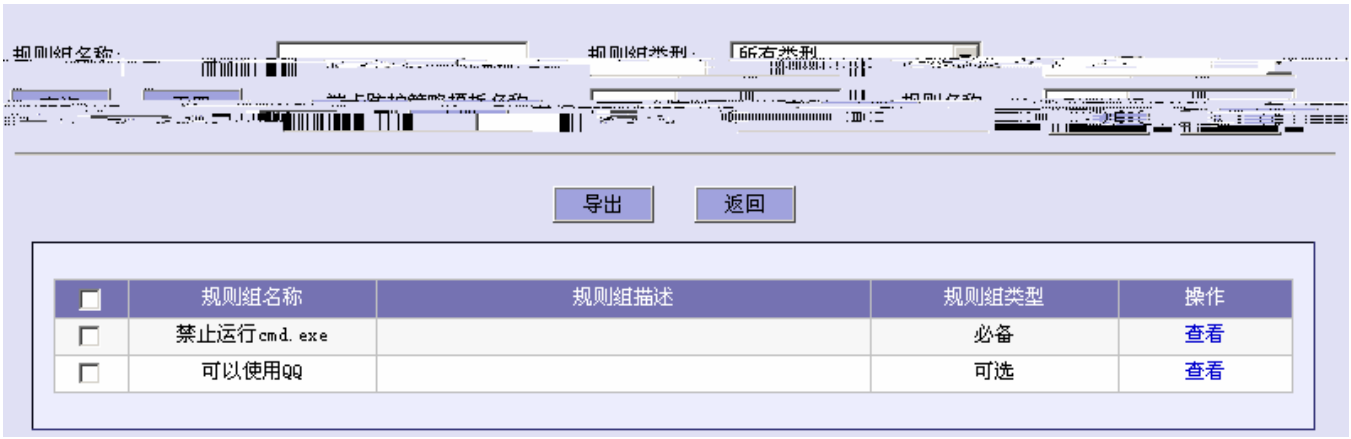
“ ” “ ”

说明

- 10M
- SMP “ ” “ ”
- “ ” “ ”

2.3.5.9

“ ” “ ” “ ” “ ” “ ”



“ ” “ ” “ ”

“ ”

“ ”

“ ” “ ”

“ ”

说明

,

, .dat

2.4

SMP

- ____
- _____
- _____
- _____
- _____
- ARP _____

2.4.1

Õ

Õ
SMP

Õ

Õ

Õ ARP ARP

2.4.2

SMP

2.4.2.1

“ ” “ ” “ ”


查询
重置
添加
删除所选
共1条记录 每页20条 第1页/共1页 GO
[首页] [上一页] [下一页] [尾页]
敏感资源IP
子网掩码
敏感资源名称
敏感资源描述
操作
192.168.203.1
255.255.255.255
核心网关
公司的核心网关
查看 修改

“ ” “ ” “

”

“ ” “ ”

ü “ ” “ ” “

”

ü “ ” “ ”

ü

ü “ ” “ ” “

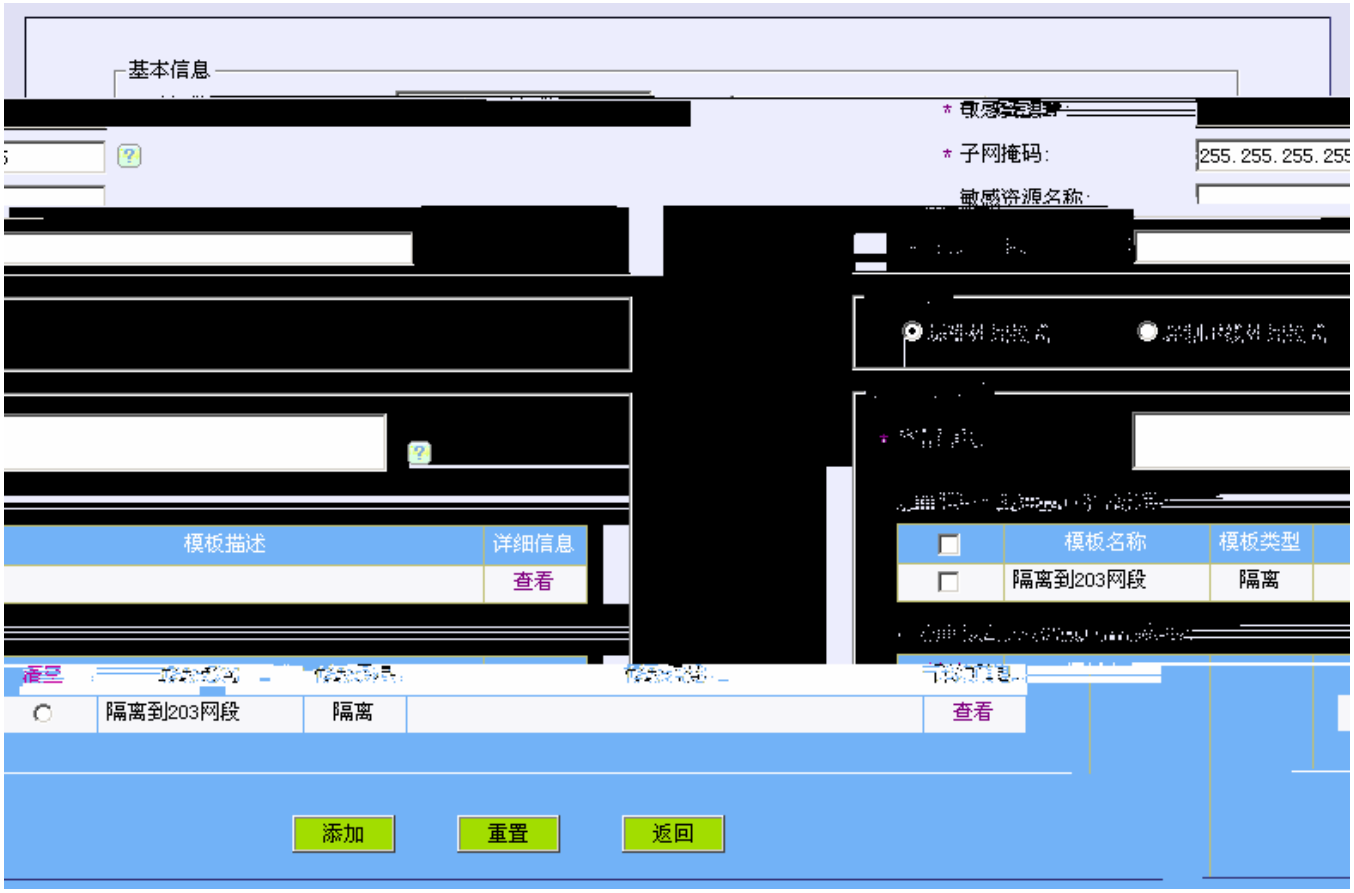
”

说明

，

2.4.2.2

“ ” “ ” “ ”


基本信息
* 子网掩码:
255. 255. 255. 255
模板描述
详细信息
查看
模板名称
模板类型
隔离到203网段
隔离
隔离到203网段
隔离
查看
添加
重置
返回

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

“*”

“ ”

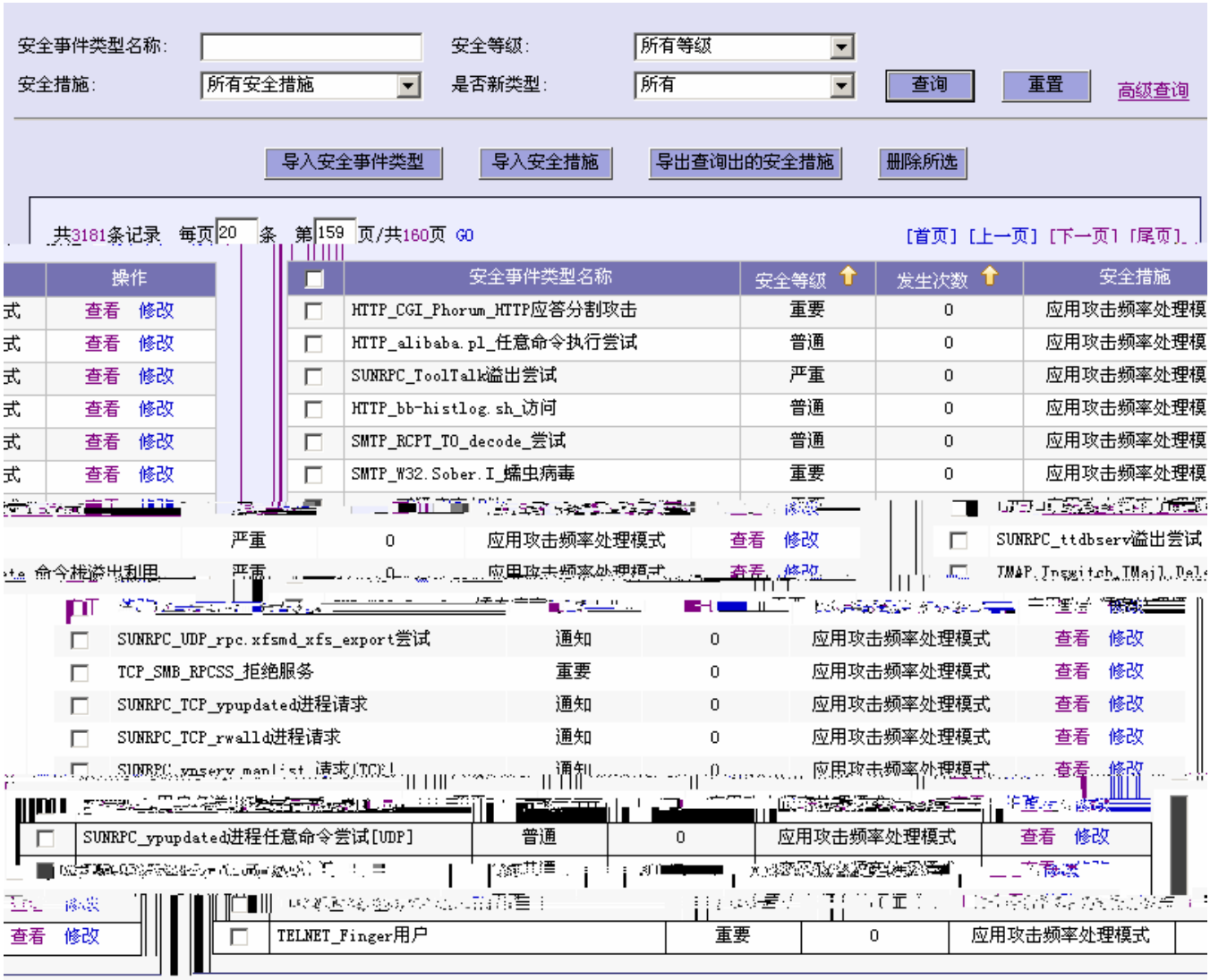
“ ”

“ ”

2.4.2.3

2.4.3.1

“ ” “ ” “ ”


安全事件类型名称:
安全等级:
所有等级
安全措施:
所有安全措施
是否新类型:
所有
查询
重置
高级查询
导入安全事件类型
导入安全措施
导出查询出的安全措施
删除所选
共3181条记录 每页20 条 第159 页/共160页 GO
[首页] [上一页] [下一页] [尾页]
操作
安全事件类型名称
安全等级
发生次数
安全措施
HTTP_CGI_Phorum_HTTP应答分割攻击 重要 0 应用攻击频率处理模
HTTP_alibaba.pl_任意命令执行尝试 普通 0 应用攻击频率处理模
SUNRPC_ToolTalk溢出尝试 严重 0 应用攻击频率处理模
HTTP_bb-histlog.sh_访问 普通 0 应用攻击频率处理模
SMTP_RCPT_TO_decode_尝试 普通 0 应用攻击频率处理模
SMTP_W32.Sober.I_蠕虫病毒 重要 0 应用攻击频率处理模
严重 0 应用攻击频率处理模式 查看 修改
SUNRPC_ttdbserv溢出尝试
SUNRPC_UDP_rpc.xfsmd_xfs_export尝试 通知 0 应用攻击频率处理模式 查看 修改
TCP_SMB_RPCSS_拒绝服务 重要 0 应用攻击频率处理模式 查看 修改
SUNRPC_TCP_ypupdated进程请求 通知 0 应用攻击频率处理模式 查看 修改
SUNRPC_TCP_rwalld进程请求 通知 0 应用攻击频率处理模式 查看 修改
SUNRPC_ypupdated进程任意命令尝试[UDP] 普通 0 应用攻击频率处理模式 查看 修改
TELNET_Finger用户 重要 0 应用攻击频率处理模式

“ ” “ ” “

”

“ ” “ ”

“ ”

ü “ ”

“ ”

ü “ ”
“ ”

ü “ ”
“ ”

ü “ ” “ ”

ü

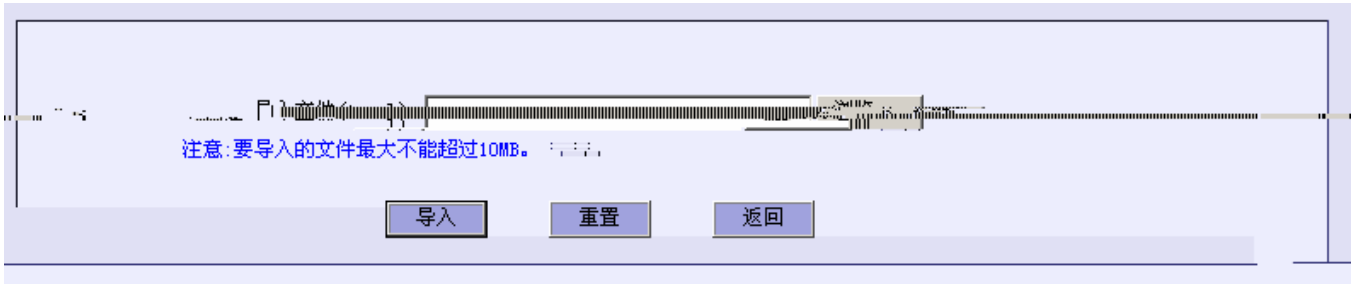
ü “ ” “ ” “
”

说明

，

2.4.3.2

“ ” “ ” “ ”



“ …”

“ ”

“ ”

“ ” “ ”

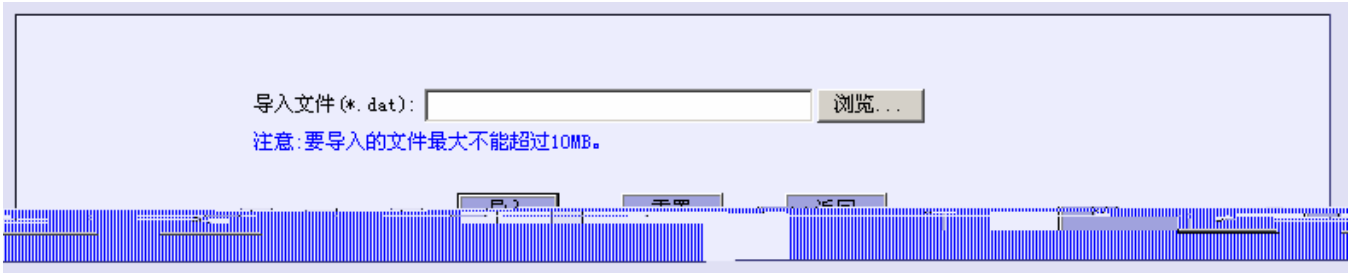
说明

， 10M

， IDS XML

2.4.3.3

“ ” “ ” “ ”



“ …”

“ ”

“ ”

“ ” “ ”

说明

, 10M

, SMP “ ”

,

2.4.3.4

“ ” “ ”

说明

.dat

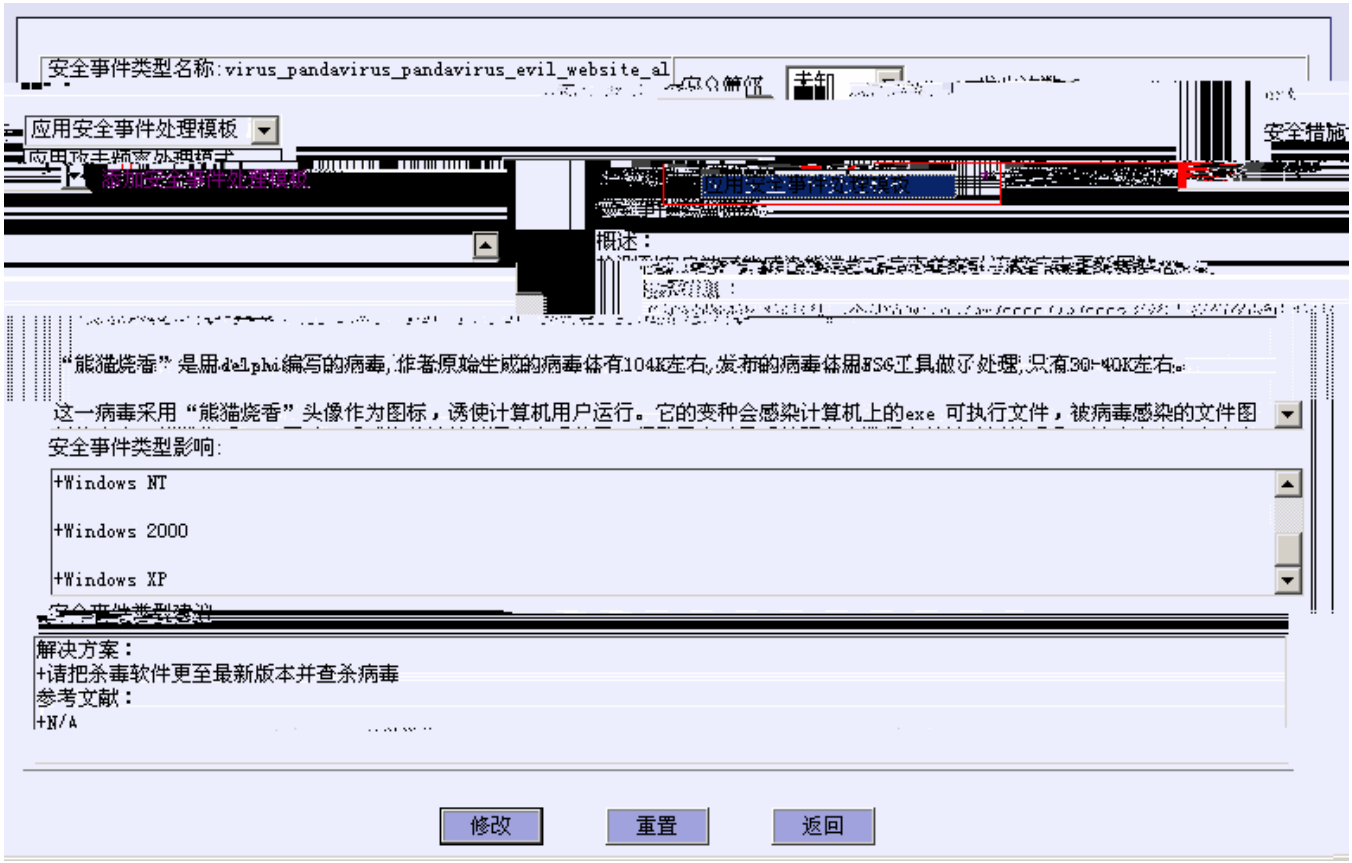
2.4.3.5

“ ” “ ” “ ”


安全事件类型名称:virus_pandavirus_pandavirus_evil_website_alert
安全等级: 未知
发生次数:0
安全措施: 应用攻击频率处理模式
安全事件类型描述:
概述：
检测到客户端可能感染熊猫烧香病毒并主动连接病毒更新网站。
技术信息：
“熊猫烧香”病毒是一个能在Win9x/NT/2000/XP/2003系统上运行的蠕虫病毒。
这一病毒采用“熊猫烧香”头像作为图标，诱使计算机用户运行。它的变种会感染计算机上的exe 可执行文件，被病毒感染的文件图
安全事件类型影响:
+Windows NT
+Windows 2000
+Windows XP
安全事件类型建议:
解决方案：
+请把杀毒软件更至最新版本并查杀病毒
参考文献：
+N/A
修改
重置
返回

“ ”

“ ” “ ”


安全事件类型名称:virus_pandavirus_pandavirus_evil_website_al
应用安全事件处理模板
概述：
“熊猫烧香”是用delphi编写的病毒，作者原始生成的病毒体有104K左右，发布的病毒体用FSG工具做了处理，只有30-40K左右。
这一病毒采用“熊猫烧香”头像作为图标，诱使计算机用户运行。它的变种会感染计算机上的exe 可执行文件，被病毒感染的文件图
安全事件类型影响:
+Windows NT
+Windows 2000
+Windows XP
解决方案：
+请把杀毒软件更至最新版本并查杀病毒
参考文献：
+N/A
修改
重置
返回

“ ”

“ ”

“ ” “ ”

“ ”

“ ”

“ ” “ ”

说明

，

“ ”

，

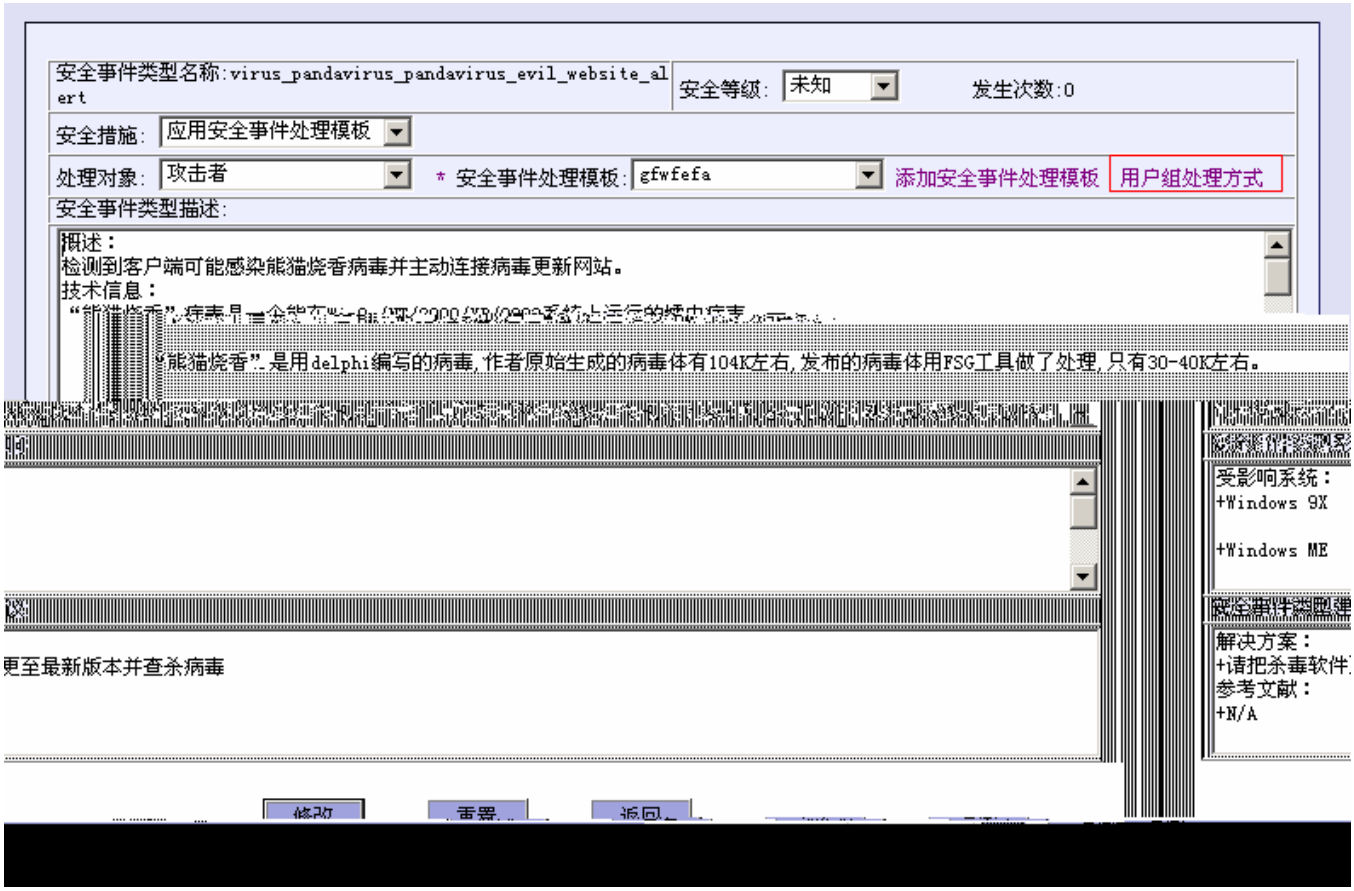
“ ” “ ”

，

2.4.3.6

“ ” “ ”

“ ”


安全事件类型名称:virus_pandavirus_pandavirus_evil_website_alert
安全等级: 未知
发生次数:0
安全措施: 应用安全事件处理模板
处理对象: 攻击者
* 安全事件处理模板: gfwfefa
添加安全事件处理模板
用户组处理方式
安全事件类型描述:
概述:
检测到客户端可能感染熊猫烧香病毒并主动连接病毒更新网站。
技术信息:
“熊猫烧香”是用delphi编写的病毒,作者原始生成的病毒体有104K左右,发布的病毒体用FSG工具做了处理,只有30-40K左右。
受影响系统:
+Windows 9X
+Windows ME
更至最新版本并查杀病毒
解决方案:
参考文献:
+N/A
修改
重置
返回

“ ”

“ ” “ ”

“ ”

“ ”

“ ” “ ”

注意

,

2.4.3.7

“ ” “ ”

说明

“ ”
，

2.4.5.1

“ ” “ ” “

”

“ ” “ ” “

”

“ ” “ ”

ü “ ” “ ”

“ ”“9ïï piU‘ ¾ ”

2.4.5.2

“ ” “ ” “ ”

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

“*” 64 32

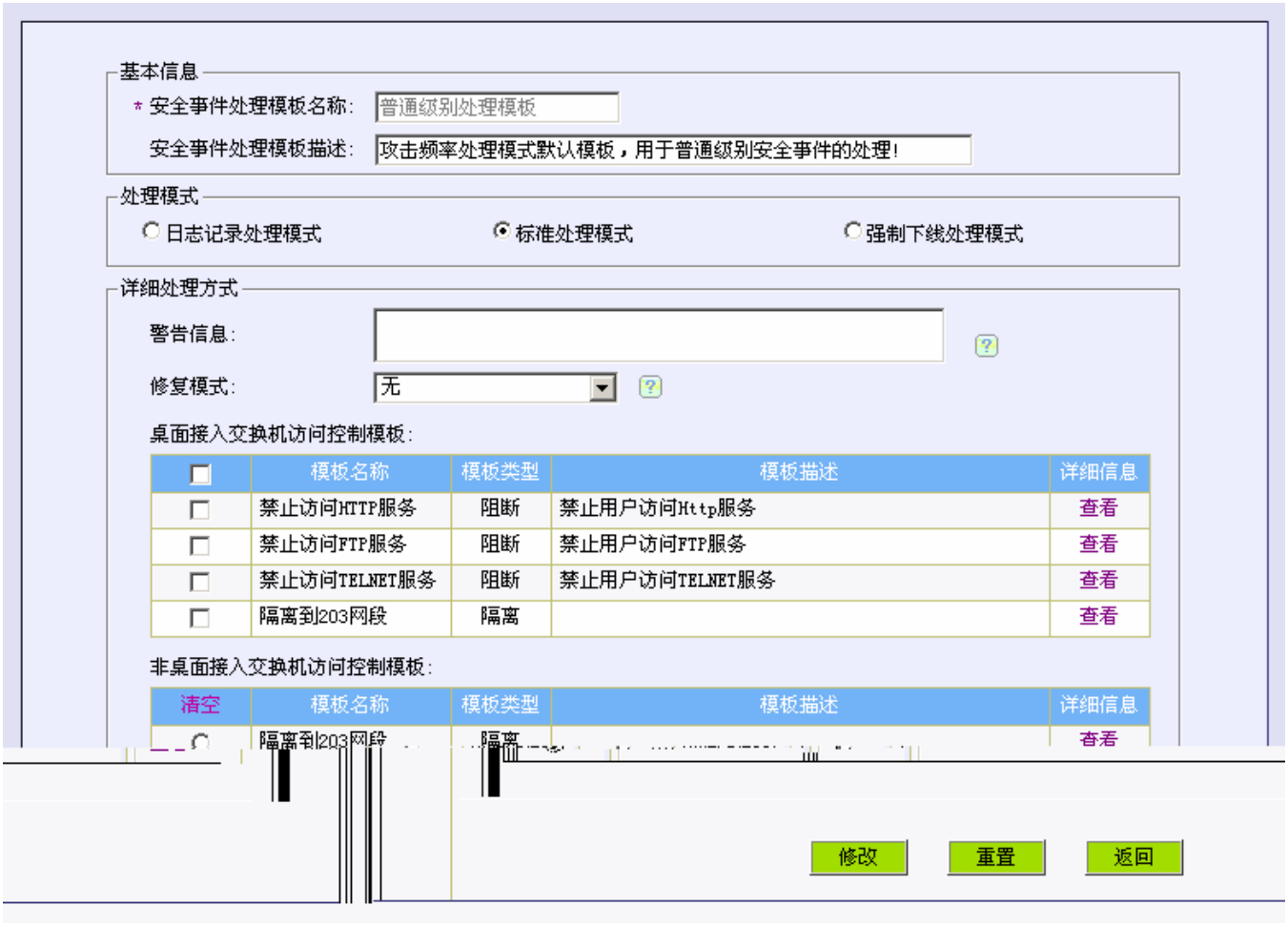
“

”

“ ”

2.4.5.3

“ ” “ ” “ ”


基本信息
* 安全事件处理模板名称: 普通级别处理模板
安全事件处理模板描述: 攻击频率处理模式默认模板，用于普通级别安全事件的处理!
处理模式
日志记录处理模式
标准处理模式
强制下线处理模式
详细处理方式
警告信息:
修复模式: 无
桌面接入交换机访问控制模板:
模板名称 模板类型 模板描述 详细信息
禁止访问HTTP服务 阻断 禁止用户访问Http服务 查看
禁止访问FTP服务 阻断 禁止用户访问FTP服务 查看
禁止访问TELNET服务 阻断 禁止用户访问TELNET服务 查看
隔离到203网段 隔离 查看
非桌面接入交换机访问控制模板:
清空 模板名称 模板类型 模板描述 详细信息
修改
重置
返回

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

。

2.4.5.4

“ ” “ ”

说明

，

2.4.6 ARP

“ ” “ARP ” “ ARP ”

“ ”

“ ARP ” ARP

“ ARP ” ARP

“ ARP ” ARP

说明

， ARP

， “ > ” ARP ARP

2.5

SMP

，

，

，

，

,

2.5.1

Õ

Õ

Õ HTTP FTP

Õ

“ ” “ ” “

”

“ ” “ ”

ü “ ” “ ” “

”

ü “ ” “ ”

ü

ü “ ”

ü “ ” “ ” “

”

说明

，

2.5.2.2

“ ” “ ” “ ”


访问控制模板名称:
目的IP:
访问控制模板类型:
所有类型
目的MAC:
目的端口:
源端口:
查询
重置
添加端点防护模板
添加隔离模板
添加阻断模板
添加上网权限模板
删除所选
访问控制模板描述
操作
访问控制模板名称
访问控制模板类型
查看 修改
隔离到203网段
隔离模板
禁止访问FTP服务
阻断模板
查看 修改
禁止访问HTTP服务
阻断模板
查看 修改
上网权限模板
查看 修改

“ ” “ ” “

”

“ ” “ ”

ü “ ” “ ”

“ ”

ü “ ” “ ” “

”

ü “ ” “ ” “

”

ü “ ” “ ”

“ ”

ü “ ” “

”

ü

ü “ ” “ ”

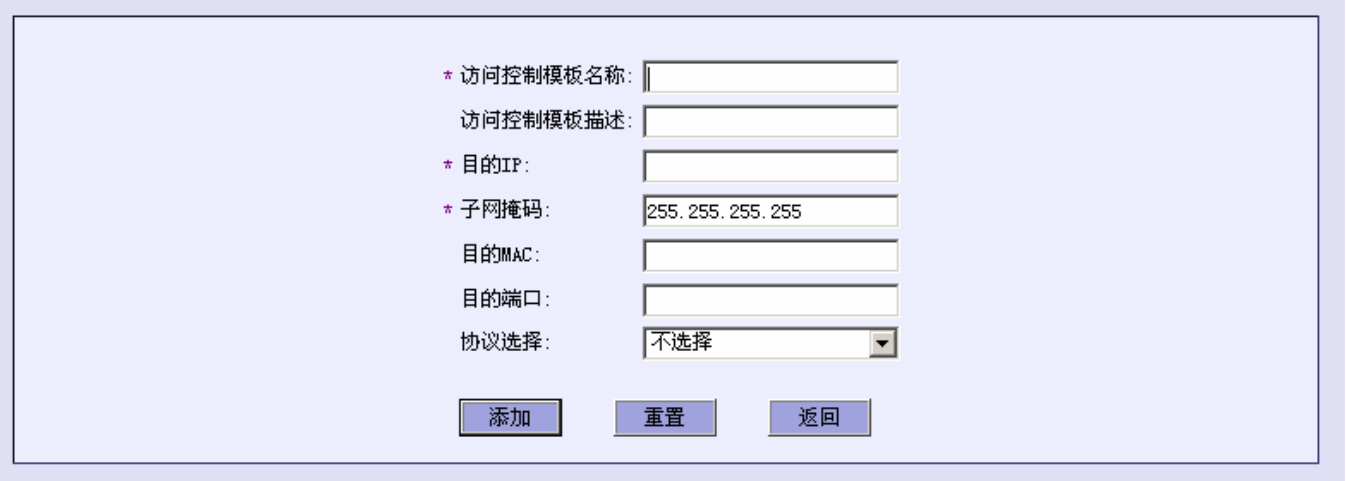
“ ”

说明

，

2.5.3.2

“ ” “ ” “ ”



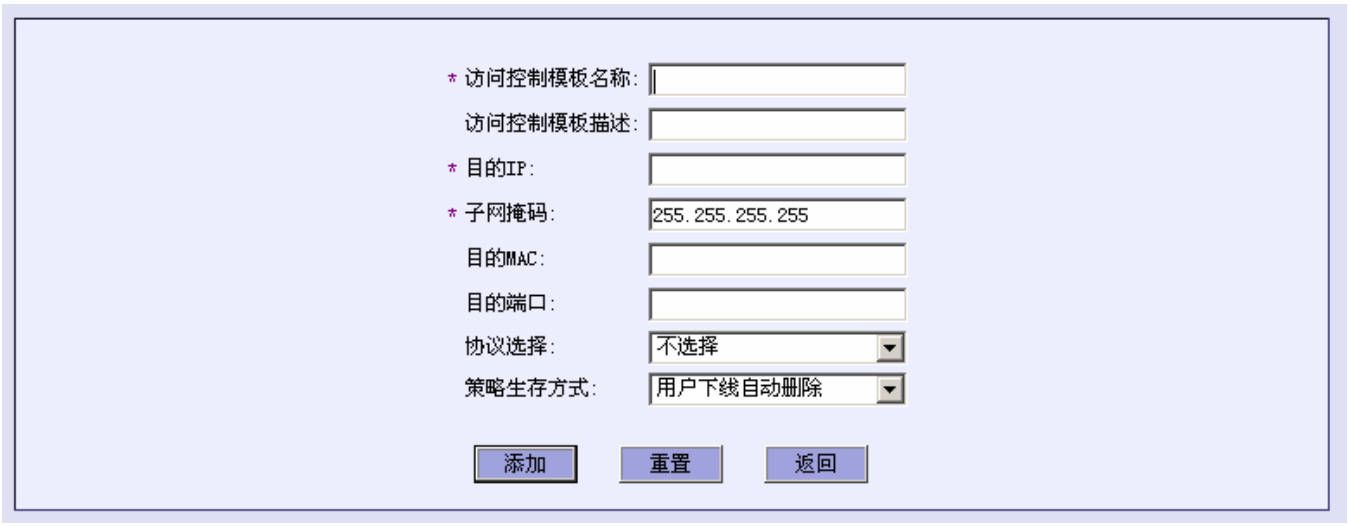
“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

93 Td <23CF087430C507 031 Tf 10.5 30 Tf


* 访问控制模板名称:
访问控制模板描述:
* 目的IP:
* 子网掩码:
255.255.255.255
目的MAC:
目的端口:
协议选择:
不选择
策略生存方式:
用户下线自动删除
添加
重置
返回

“ ”

“ ” “ ” “ ”

“ ”

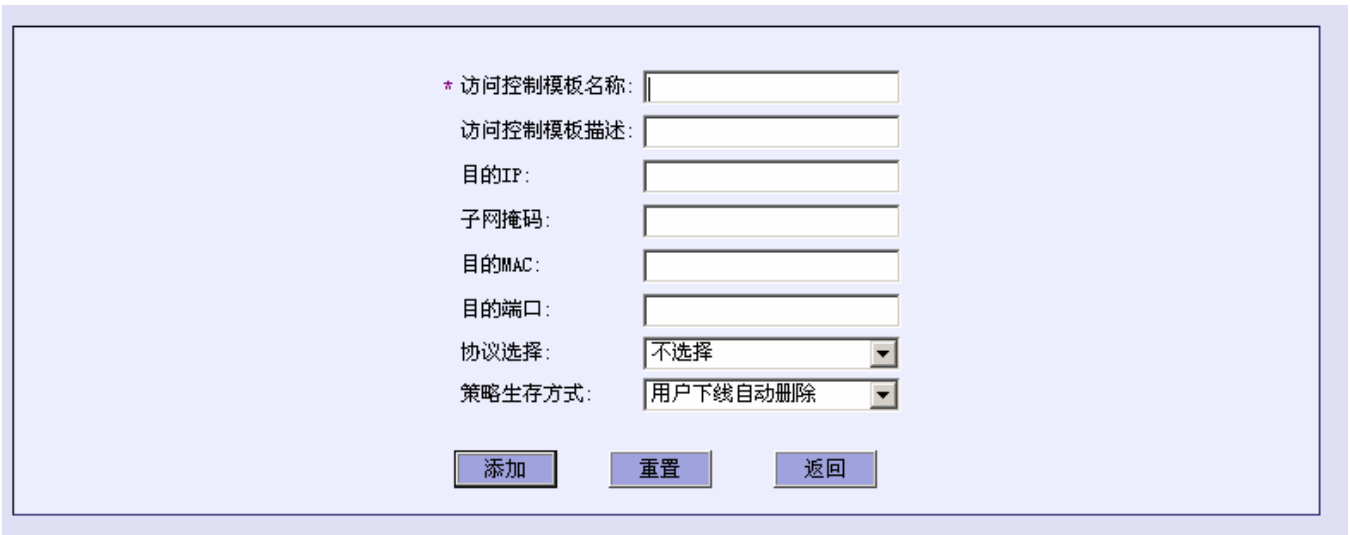
“ ” “ ”

说明

“*” 32 16

2.5.3.4

“ ” “ ” “ ”


* 访问控制模板名称:
访问控制模板描述:
目的IP:
子网掩码:
目的MAC:
目的端口:
协议选择:
不选择
策略生存方式:
用户下线自动删除
添加
重置
返回

“ ”

“ ” “ ” “ ”

“ ”

“ ” “ ”

说明

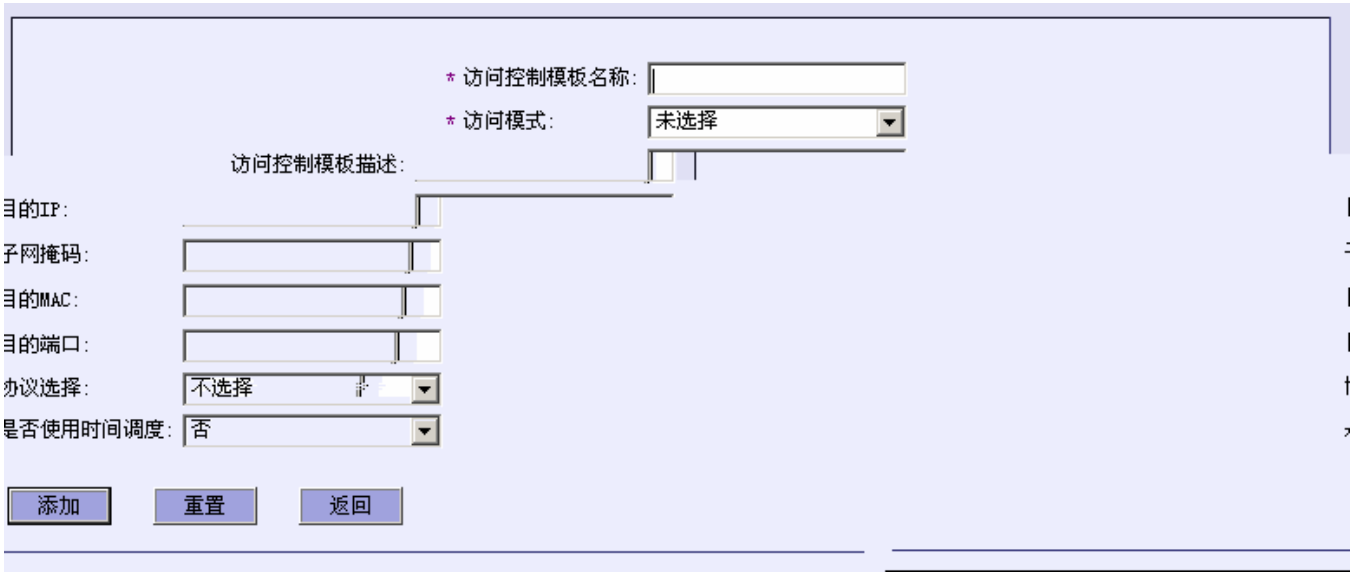
“*” 32 16

,

,

2.5.3.5

“ ” “ ” “ ”



“ ”

“ ” “ ” “

”

“ ”

“ ” “ ”

说明

“*” 32 16

“ ” “ ”

“ ”

2.5.3.6

“ ” “ ” “ ”

“ ”

“ ” “ ” “ ”

“ ”

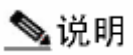
“ ” “ ”

“ ” “ ” “ ”

“ ” “ ”

2.5.3.7

“ ” “ ”



2.5.4

SMP

2.5.4.1

“ ” “ ” “

”

“ ” “ ” “

”

“ ” “ ”

ü “ ” “ ”

“ ”

ü “ ” “

”

ü

ü “ ” “ ”

“ ”

说明

。

2.5.4.2

“ ” “ ” “ ”

“ ”

“ ”

“ ”

“ ” “ ”

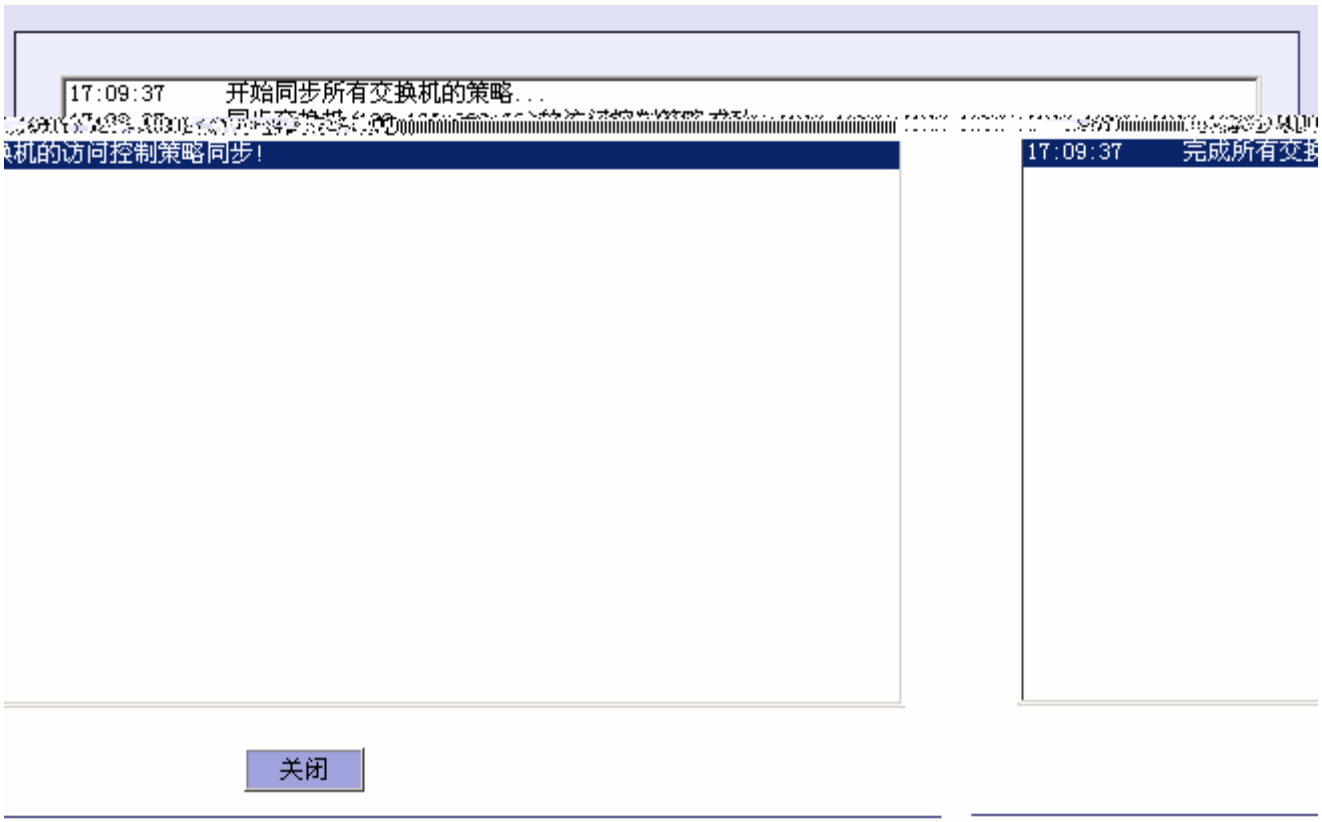
说明

- “*” 32 16
-
-

2.5.4.3

“ ” “ ” “ ”


基本信息
* 访问控制模板组名称:
禁止访问网络
访问控制模板组描述:
访问控制模板
访问控制模板名称
访问控制模板类型
访问控制模板描述
详细信息
隔离到203网段
隔离
查看
禁止访问TELNET服务
阻断
禁止用户访问TELNET服务
查看
禁止访问FTP服务
阻断
禁止用户访问FTP服务
查看
修改
重置
返回



说明

，

2.6

SMP

- ，
- ，
- ，
- ，

2.6.1

Õ

Õ MAC

Õ

Õ

Õ

2.6.2

2.6.2.1

“ ” “ ” “

”

“ ” “ ” “

”

“ ” “ ”

ü “ ” “

”

ü “ ” “

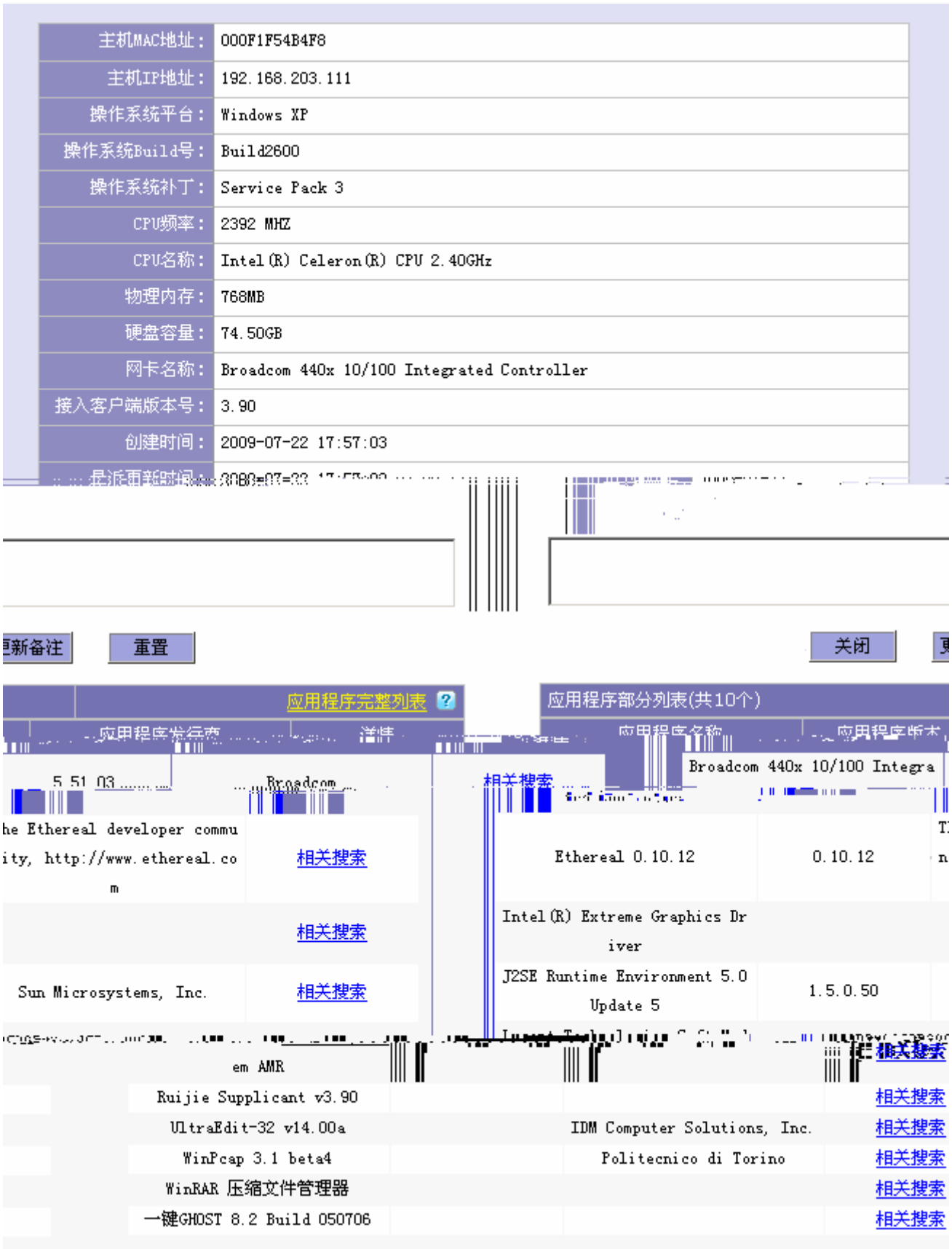
”

ü

ü “ ” “ ”

2.6.2.2

“ ” “ ” “ ”



主机MAC地址：	000F1F54B4F8
主机IP地址：	192.168.203.111
操作系统平台：	Windows XP
操作系统Build号：	Build2600
操作系统补丁：	Service Pack 3
CPU频率：	2392 MHZ
CPU名称：	Intel(R) Celeron(R) CPU 2.40GHz
物理内存：	768MB
硬盘容量：	74.50GB
网卡名称：	Broadcom 440x 10/100 Integrated Controller
接入客户端版本号：	3.90
创建时间：	2009-07-22 17:57:03

”

“ ”

“ ” “ ”

”

“ ” “ ”

ü “ ” “ ”

ü “ ” “ ” ”

ü

ü “ ” “ ” “ ”

ü “ ” “ ”

ü “ ” google

说明

，

2.6.3.2

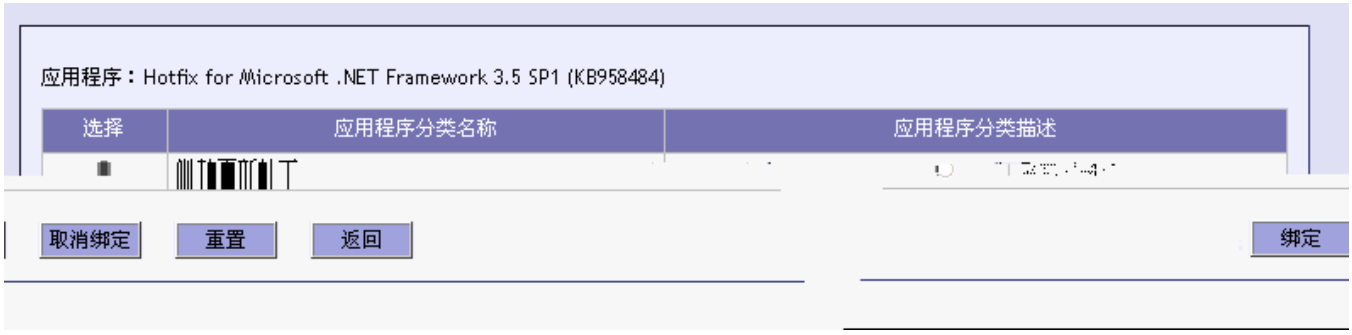
“ ” “ ”

“ ” “ ”

2.6.3.3

“ ” “ ” “ ”

”



“ ” “ ” “ ”

“ ”

“ ” “ ”

“ ”

“ ” “ ”

2.6.4

2.6.4.1

“ ” “ ” “

”

“ ” “ ” “

”

“ ” “ ”

- ü “ ” “ ”
- ü
- ü “ ” “ ” “ ”
- ü “ ” “ ” “ ”
- ü “ ” “ ”
- ü “ ” “ ” “ ”

说明

›

2.6.4.2

“ ” “ ” “ ”

“ ” “ ”

“ ” “ ”

“ ”

“ ” “ ”

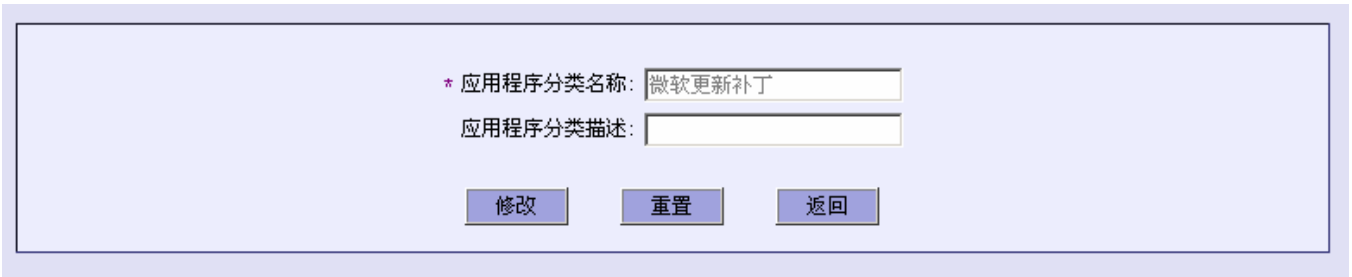
说明

“*”

›

2.6.4.3

“ ” “ ” “ ”



“ ” “ ” “ ”

“ ”

“ ” ”

“ ” “ ”

2.6.4.5

“ ” “ ”

2.7

SMP

- ____
- _____
- _____

2.7.1

SNMP

Õ SMP SMP

Õ SMP ARP

Õ

Õ [comm word]34A5116E1DA403FE1FF50/Cw54B926

“ ” “ ”

“ ” “ ”

“ ” “ ”

“ ”

ü “ ” “ ” “ ”

ü “ ” “ ” “ ”

ü “ ”

“ ”

ü “ ”

ü “ MAC” MAC

ü

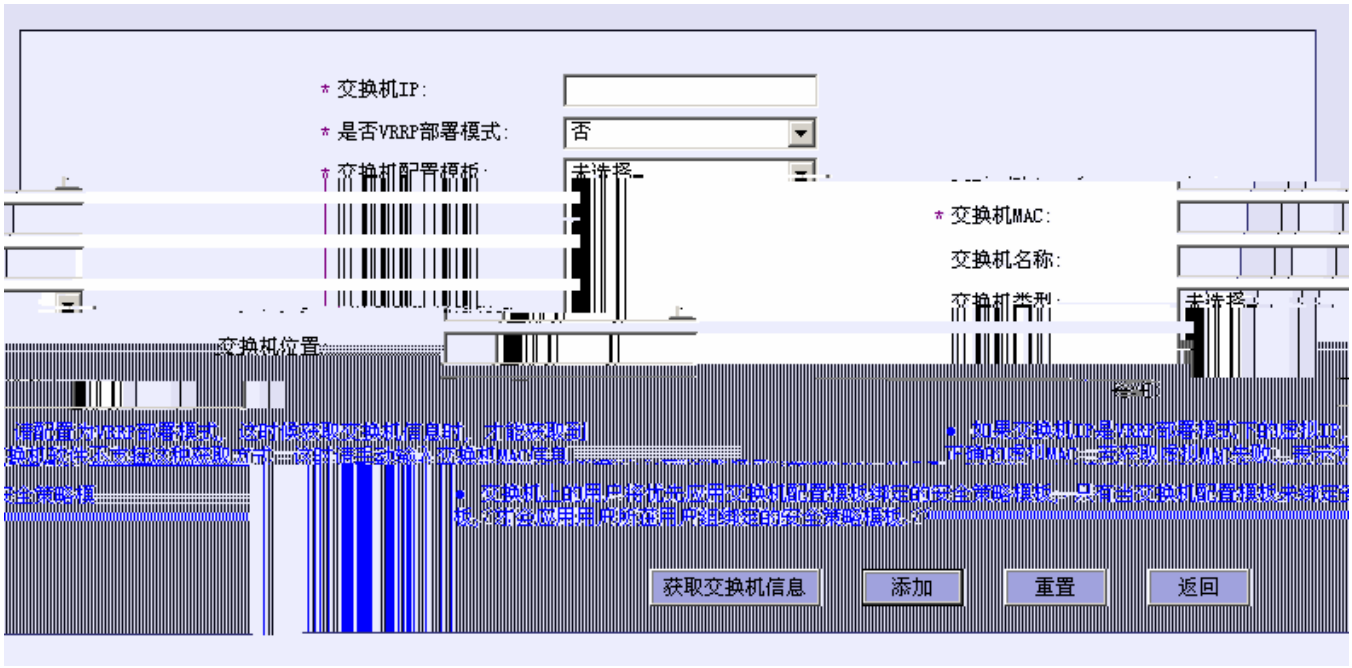
ü “ ”

ü “ ” “ ” “ ”

ü “ ” “ ”

2.7.2.2

“ ” “ ” “ ”



“ ” IP “ ”

“ ” “ ”

“ ”

“ ” “ ”

说明

“*”

，

“ ” “ ” ARP

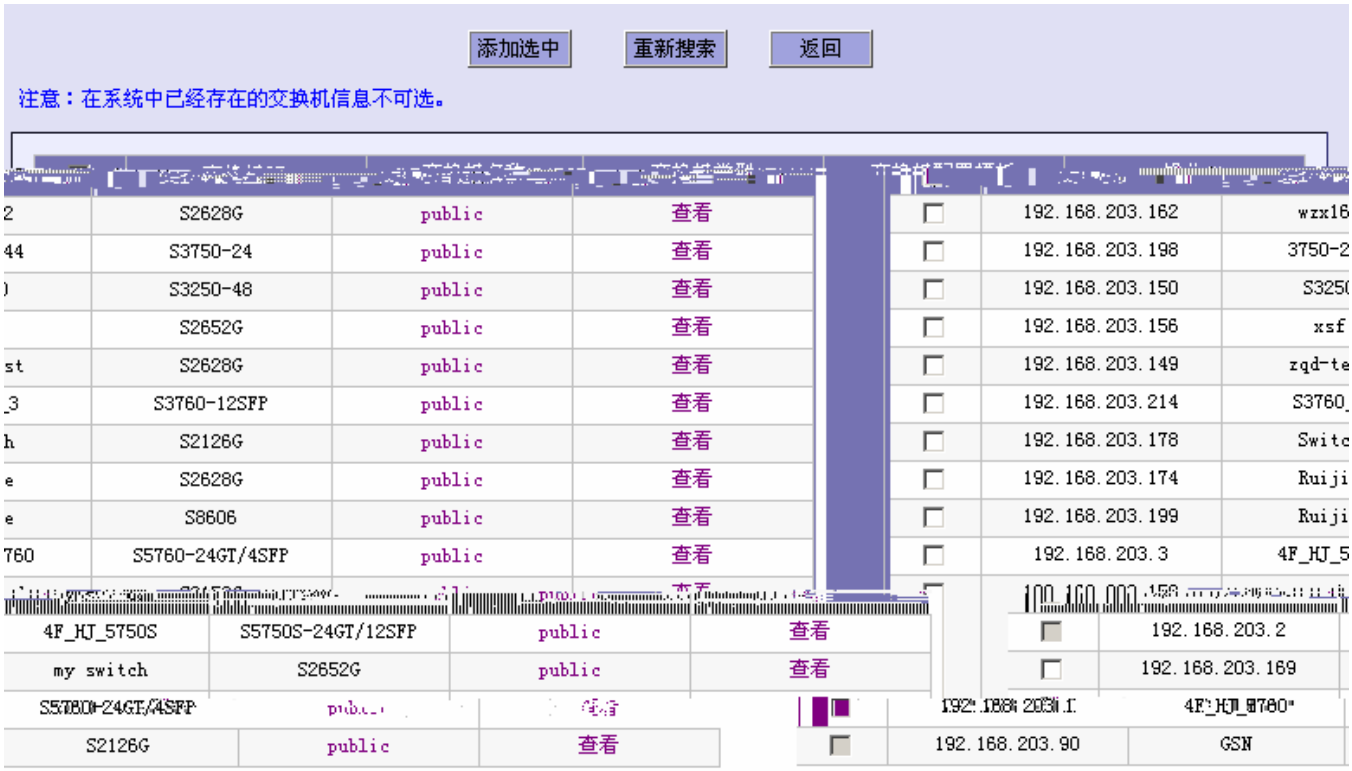
，

“ ” “ARP ” “ARP ”

ARP

2.7.2.3

“ ” “ ” “ ”


添加选中
重新搜索
返回
注意：在系统中已经存在的交换机信息不可选。
2 S2628G public 查看 192.168.203.162 wzx16
44 S3750-24 public 查看 192.168.203.198 3750-2
) S3250-48 public 查看 192.168.203.150 S3250
S2652G public 查看 192.168.203.156 xsf
st S2628G public 查看 192.168.203.149 zqd-te
3 S3760-12SFP public 查看 192.168.203.214 S3760
h S2126G public 查看 192.168.203.178 Switc
e S2628G public 查看 192.168.203.174 Ruiji
e S8606 public 查看 192.168.203.199 Ruiji
760 S5760-24GT/4SFP public 查看 192.168.203.3 4F_HJ_5
4F_HJ_5750S S5750S-24GT/12SFP public 查看 192.168.203.2
my switch S2652G public 查看 192.168.203.169
S2126G public 查看 192.168.203.90 GSN

“ ” “ ”

“ ” “ ”

“ ” “ ”

“ ”

“ ”

说明

“*”

2.7.2.4

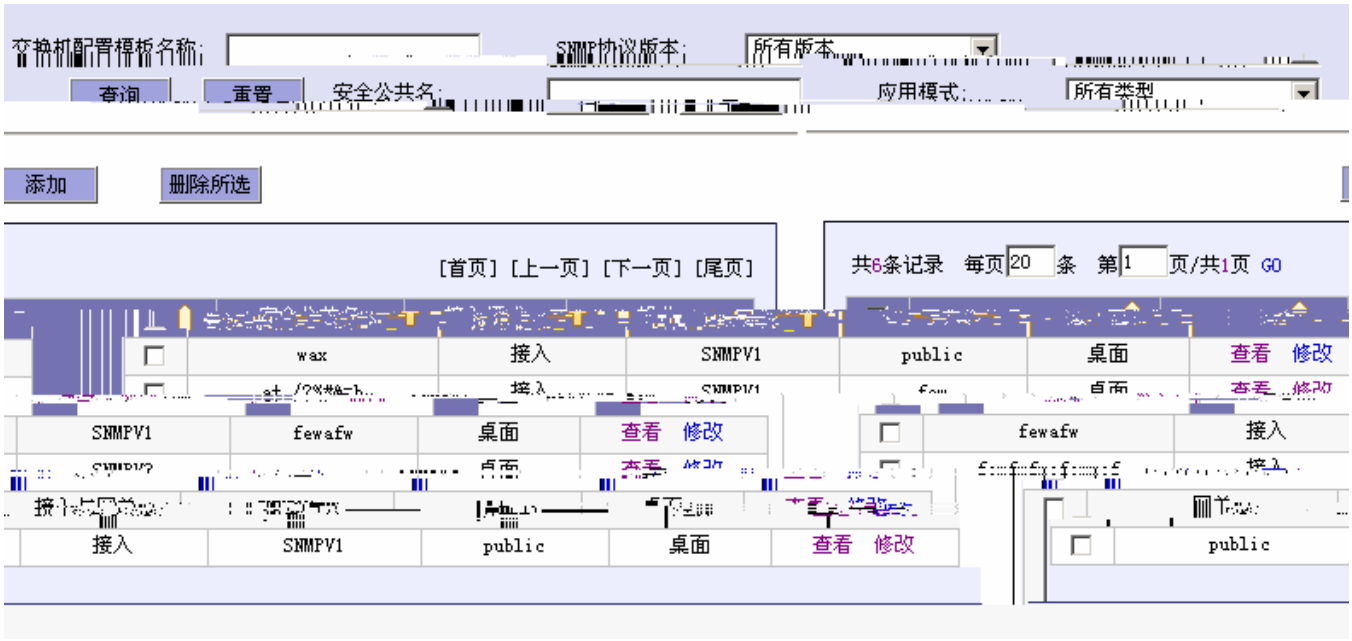
“ ” “ ” “ ”

2.7.3

2.7.3.1

“ ” “ ” “

”



“ ” “ ” “

”

“ ” “ ”

ü “ ” “

”

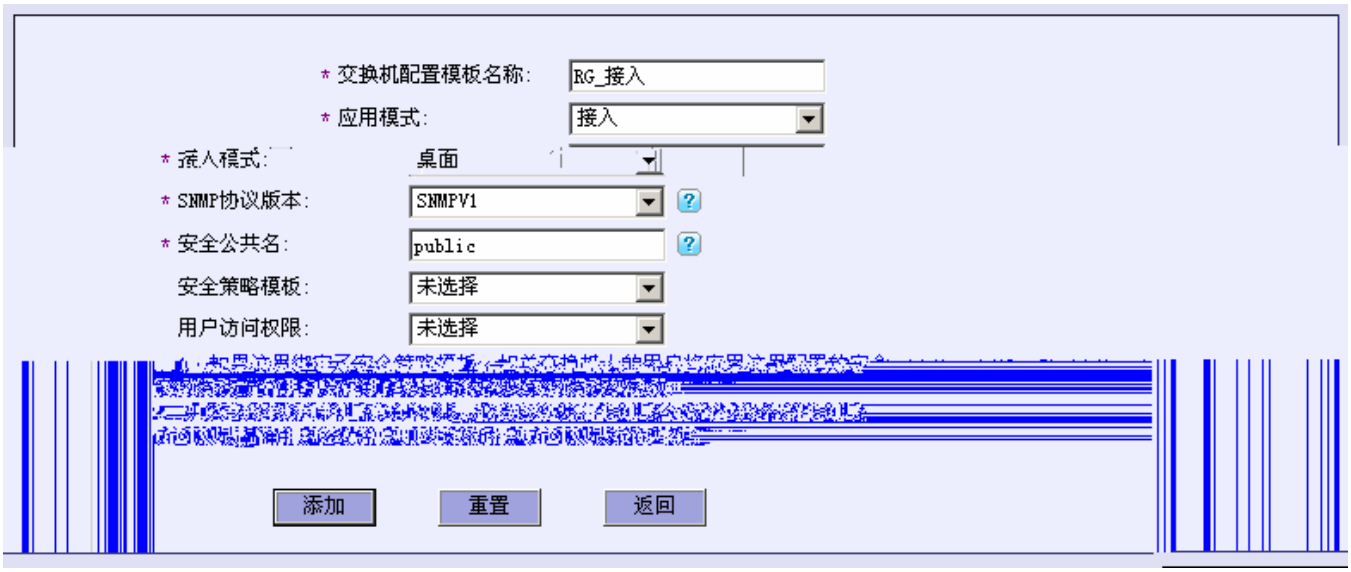
ü “ ” “ ” “ ”

ü

ü “ ” “ ” “ ”

2.7.3.2

“ ” “ ” “ ”


* 交换机配置模板名称:
RG_接入
* 应用模式:
接入
* 接入模式:
桌面
* SNMP协议版本:
SNMPV1
* 安全公共名:
public
安全策略模板:
未选择
用户访问权限:
未选择
添加
重置
返回

“ ” “ ”

“ ”

“ ”

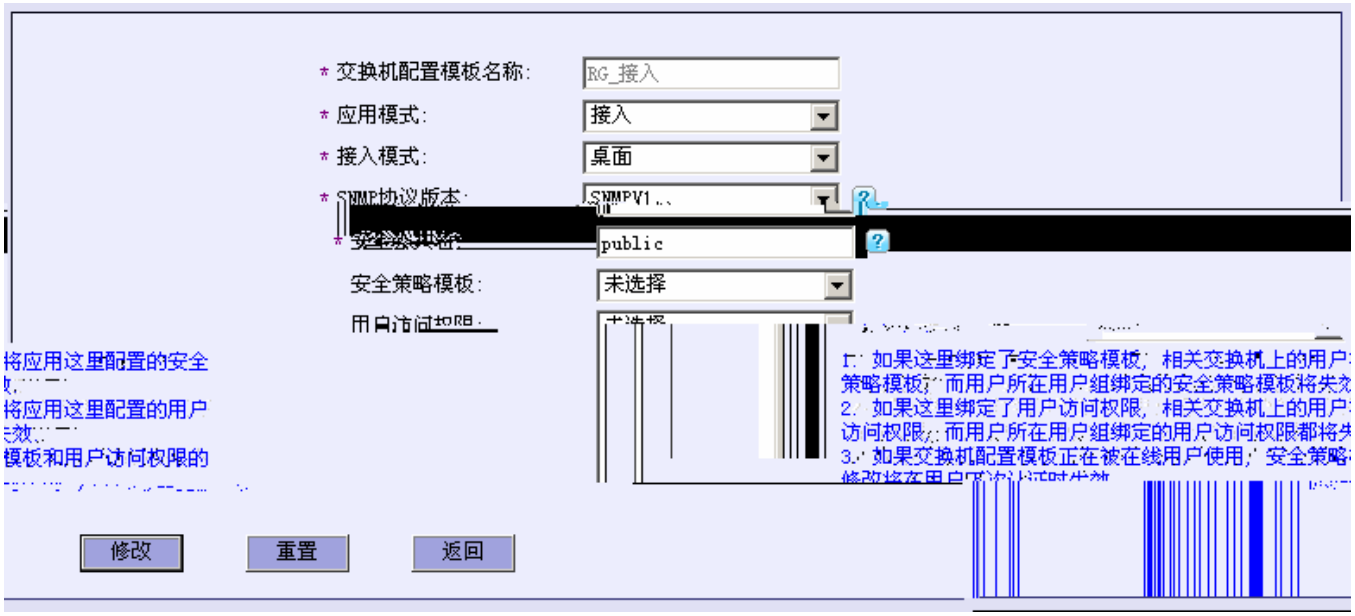
“ ” “ ”

说明

“*” 64 32

2.7.3.3

“ ” “ ” “ ”


* 交换机配置模板名称:
RG_接入
* 应用模式:
接入
* 接入模式:
桌面
* SNMP协议版本:
SNMPV1
public
安全策略模板:
未选择
用户访问权限:
修改
重置
返回

“ ” “ ”

“ ”

“ ”

“ ” “ ”

说明

“*”

。

2.7.3.4

“ ” “ ”

说明

。

A7 [illegible]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

2.8.1

Õ

Õ SMP SQL Server

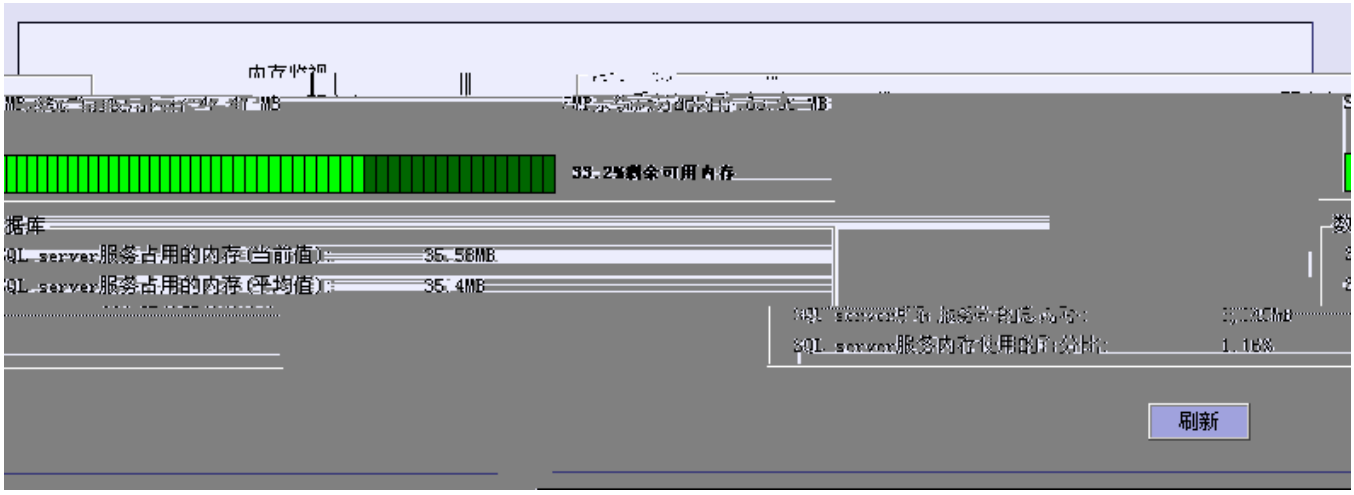
Õ

Õ

说明

2.8.2 [redacted]

“ ” “ ” “ ”


内存监视
33.2%剩余可用内存
据库
QL server服务占用的内存(当前值):
35.58MB
QL server服务占用的内存(平均值):
35.4MB
刷新

“ ”

2.8.4

“ ” “

2.8.5

“ ” “ ” “

”

“ ”

“Telnet” telnet

“ ” “ ” “ ”

“ ” “ ” “

”

“ ”

2.9

SMP

- [ ]
- [ ]

2.9.1

Õ SMP SMP

Õ SAM IP SMP

Õ SMP

Õ

Õ

Õ IP SMP
IP “ ” 127.0.0.1 192.168.1.2 127.0.0.1

Õ SMP SMP
/ / 9090

Õ 5

Õ
120

Õ SMP SMP
SMP 60

Õ

2.9.2

“ ” “ ” SMP

“ ” “ ” “ ”

“ ” “ ”

2.10

SMP

- [redacted]
- [redacted]

2.10.1

SMP

Õ “ ”

Õ “ ”

Õ “ ”

Õ “ ” SMP

Õ “ ”

Õ “ ”

Õ

Õ

Õ SMP “system”

Õ

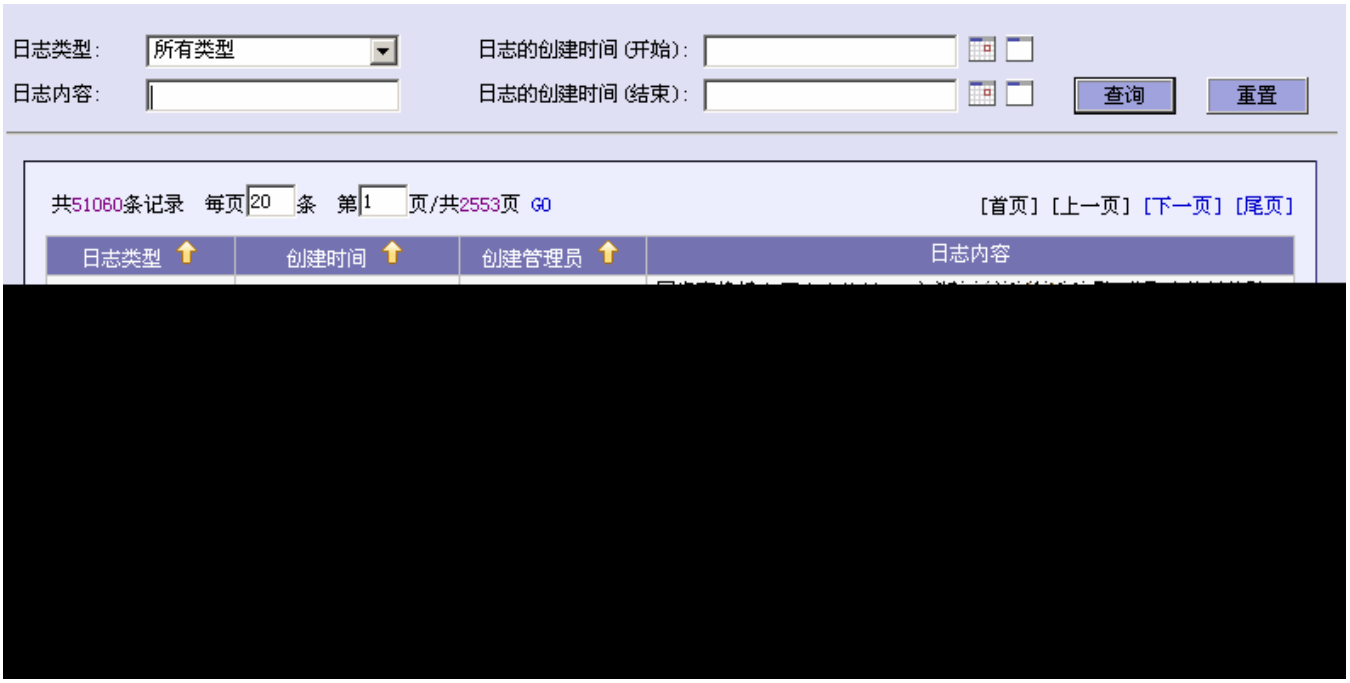
说明

,

2.10.2

2.10.2.1

“ ” “ ”


日志类型:
所有类型
日志的创建时间 (开始):
日志内容:
日志的创建时间 (结束):
查询
重置
共51060条记录 每页20 条 第1 页/共2553页 GO
[首页] [上一页] [下一页] [尾页]
日志类型
创建时间
创建管理员
日志内容

“ ” “ ”

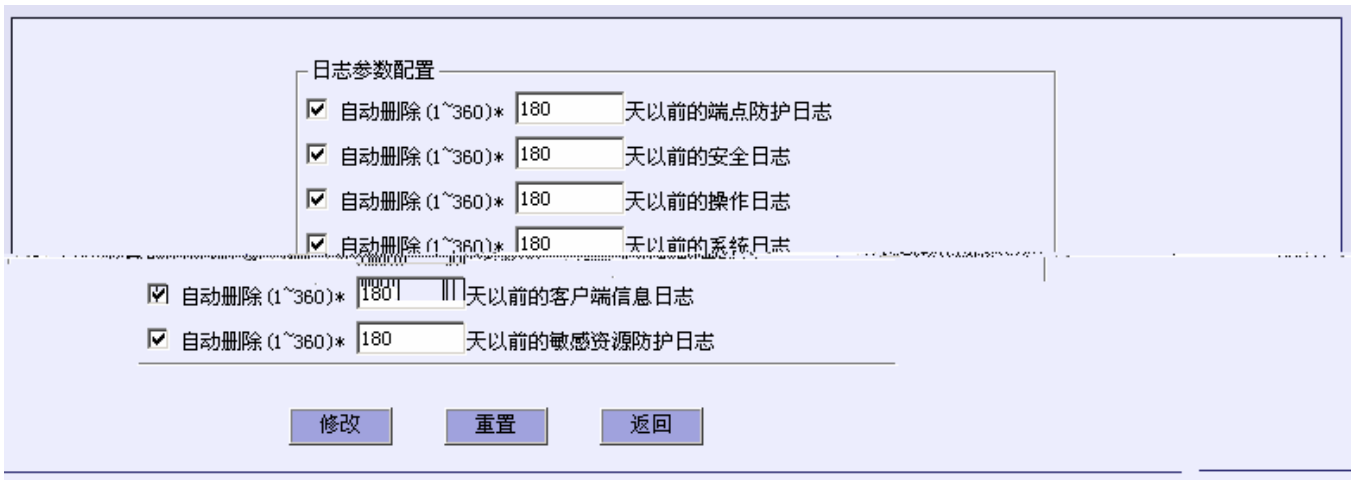
“ ” “ ”

说明

，

2.10.2.2

“ ” “ ”


日志参数配置
自动删除(1~360)* 180 天以前的端点防护日志
自动删除(1~360)* 180 天以前的安全日志
自动删除(1~360)* 180 天以前的操作日志
自动删除(1~360)* 180 天以前的系统日志
自动删除(1~360)* 180 天以前的客户端信息日志
自动删除(1~360)* 180 天以前的敏感资源防护日志
修改
重置
返回

“ ” “ ” “

”

“ ”

“ ” “ ”

说明

，

2.11.1

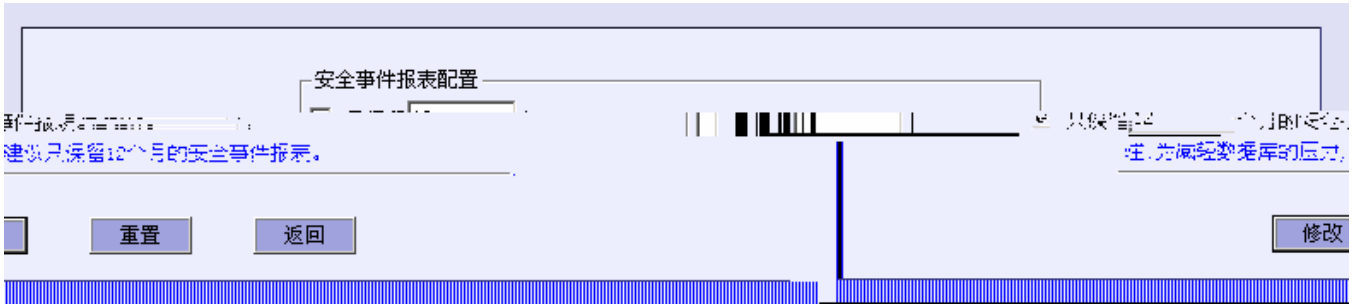
- Õ
- Õ
- Õ
- Õ TOP N
- Õ TOP N
- Õ
- Õ
- Õ TOP
- Õ TOP

2.11.2

2.11.2.1

“ ” “ ”

“ ” “ ” “ ”



“ ” “

”

“ ”

“ ”

说明

， 12

2.11.2.2

“ ” “ ”

“ ” “ ” “ ”

“ ” “ ”

“ ”

“ ” “ ”

说明

，

，

2.11.2.3

“ ” “ ”

“ ” “ ” “ ”


结束日期:
2009-07-15
安全事件类型TOP:
(默认值为10)
交换机TOP:
(默认值为10)
生成报表
重置
返回

“ ” “ ”

“ ”

“ ” “ ”

说明

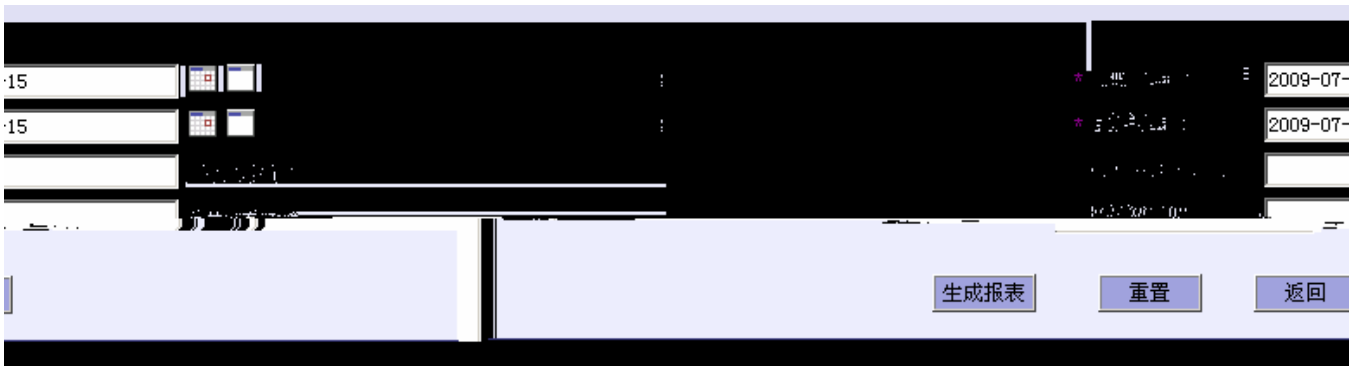
,

,

2.11.2.4

“ ” “ ”

“ ” “ ” “ ”


15
15
2009-07-
2009-07-
生成报表
重置
返回

“ ” “ ”

“ ”

“ ” “ ”

说明

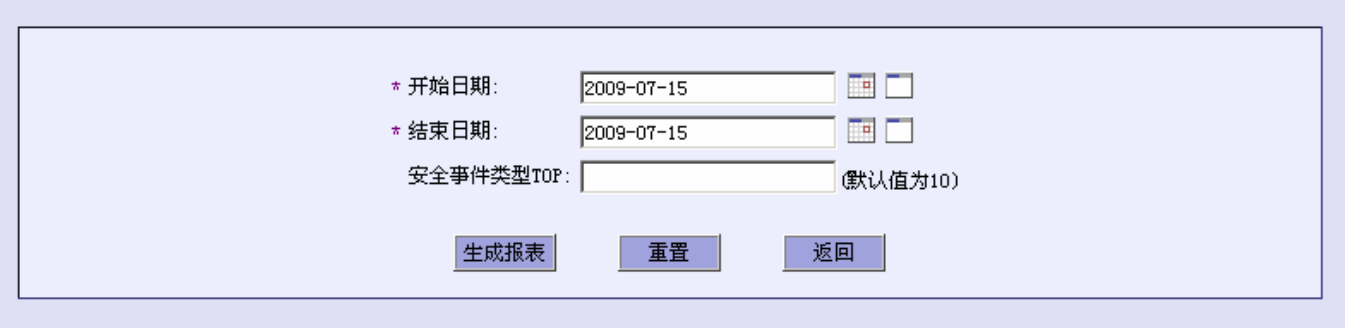
，

，

2.11.2.5 ( )

“ ” “ ”

“ ” “ ( )” “ ( )”



“ ( )” ( )

“ ” N

“ ”

“ ” “ ”

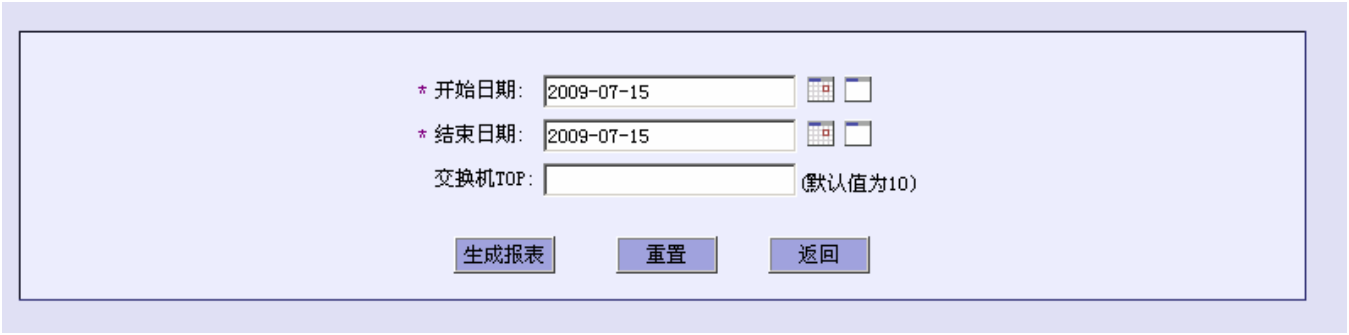
说明

，

2.11.2.6 ( )

“ ” “ ”

“ ” “ ( )” “ ( )”


* 开始日期: 2009-07-15
* 结束日期: 2009-07-15
交换机TOP:
(默认值为10)
生成报表
重置
返回

“ ( )” ( ) “

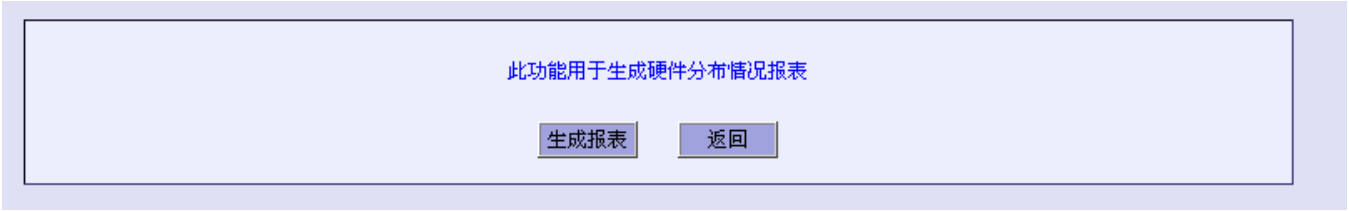
”

说明

，

2.11.2.8

“ ” “ ” “ ”



“ ” “ ”

“ ” “ ”

3 FAQ

1.

SMP http://127.0.0.1:8080/smp/index.jsp
admin 111111111

2.

SMP

IP

3. SMP HTTP HTTPS

SMP “ / ”
HTTP HTTPS

4. **“ ” session**

SMP IE “ ” “ ”

IE SMP

5. **“ ” session**

SMP

`	~	!	@	#	$	%	^	&	*
(	)			[	]	{	}		
_	-	=	+	,	.				
;	:	“	”	‘	’	<	>		
‘	’	“	”	…	‰				