

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



©2009



RGOS® RGNOS®



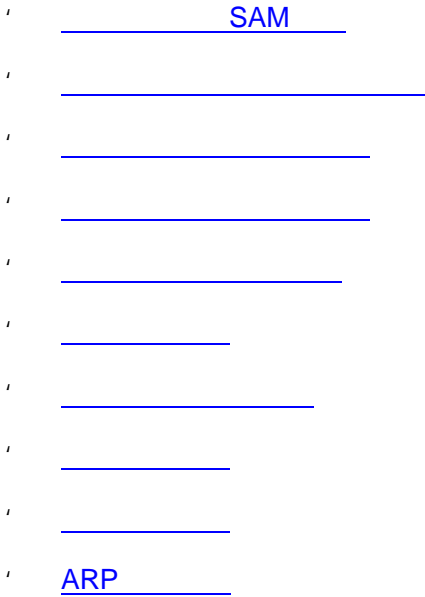
Red-Giant®



.....

1

RG-SMP



1.1 SAM

SAM

SAM

RG-SMP

1.1.1

%

“

»

”

“

”

* 交换机配置模板名称:

* 应用模式:

* 接入模式:

* SNMP协议版本: ?

* 安全公共名: ?

安全策略模板:

用户访问权限:

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.

& “ ”

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:

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: 分钟 (默认为60分钟)

* 配置文件更新服务器:

网络攻击防治

开启网络攻击防治

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 <= % 时直接丢弃

* 可信度 <= % 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 <= % 时直接丢弃

* 可信度 <= % 时只记录日志

* 安全事件解析器IP:

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, 192.168.2.23”。

其他功能

* 第三方系统访问端口: (默认)

* 端点防护状态检测周期: 分钟

* 软硬件配置信息报告周期: 分钟

* 修复服务器:

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。

&

“ ”

1.2

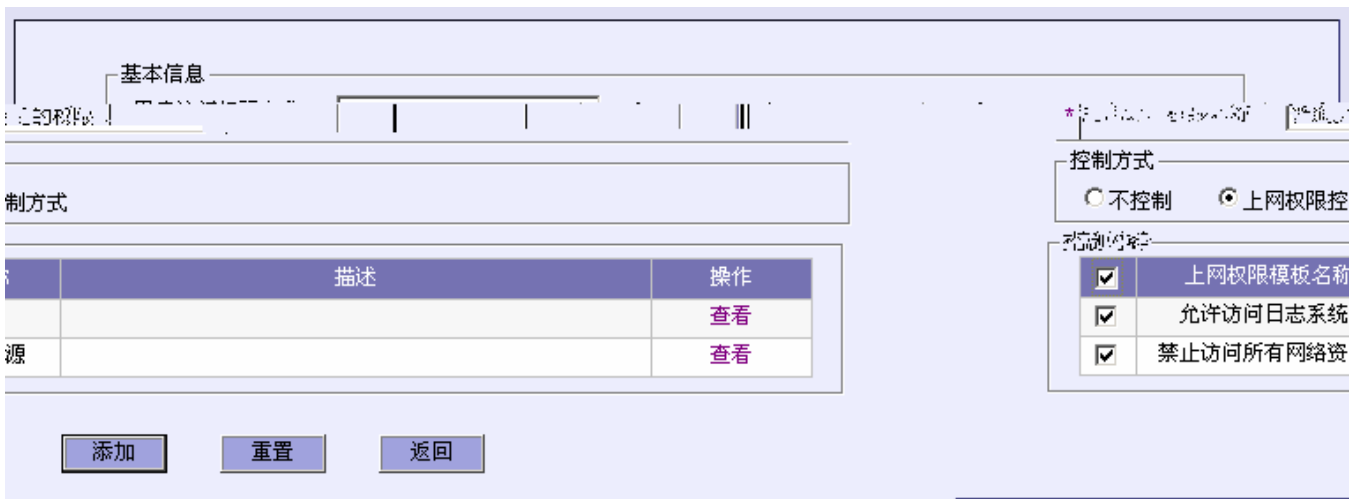
RG-SMP

1.2.1

[1.1](#)

1.2.2

% “ > ” “ ”



描述	操作
	查看
源	查看

控制方式
 不控制 上网权限控

控制策略

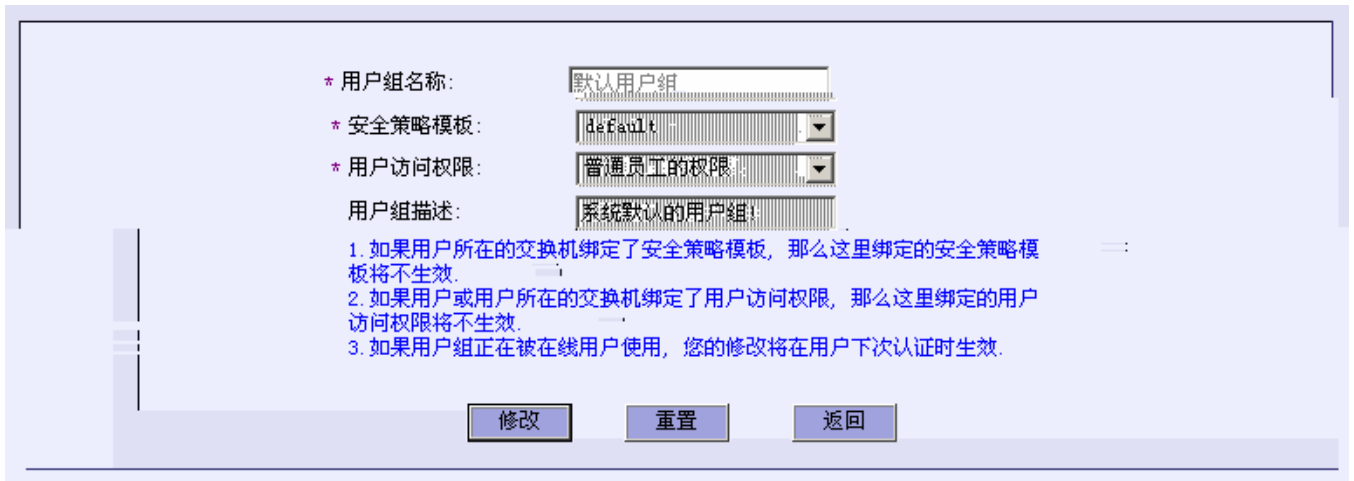
<input checked="" type="checkbox"/>	上网权限模板名称
<input checked="" type="checkbox"/>	允许访问日志系统
<input checked="" type="checkbox"/>	禁止访问所有网络资

添加 重置 返回

& “ ”

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
不检查			<input checked="" type="checkbox"/>	查看 修改	江民2006及以下的版本	弱联动	杀毒引擎 病毒库
检查	自适应顺延天数	7					
不检查			<input type="checkbox"/>	查看 修改	江民杀毒软件KV2007	弱联动	杀毒引擎 病毒库
检查	自适应顺延天数	7					
不支持			<input type="checkbox"/>	查看 修改			杀毒引擎
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			<input type="checkbox"/>	查看 修改
		病毒库	检查	自适应顺延天数	7		
卡斯基反病毒7.0个人版	弱联动	杀毒引擎	不支持			<input type="checkbox"/>	查看 修改
		病毒库	检查	自适应顺延天数	7		
		杀毒引擎	不支持				
		Symantec AntiVirus企业版 8	弱联动	杀毒引擎	不检查		
				病毒库	检查	自适应顺延天数	7
		Symantec AntiVirus企业版 9	弱联动	杀毒引擎	不检查		
iVirus企业版 10	弱联动	杀毒引擎	不检查			<input type="checkbox"/>	查看 修改
		病毒库	检查	自适应顺延天数	7		Symantec Ant
V3 VirusBlock2005	弱联动	杀毒引擎	检查	自适应顺延天数	7	<input type="checkbox"/>	查看 修改
		病毒库	不支持				安博士杀毒软件
an V10.0	弱联动	杀毒引擎	不检查			<input type="checkbox"/>	查看 修改
		病毒库	不检查				
erprise 8.5.0i	弱联动	杀毒引擎	不检查			<input type="checkbox"/>	查看 修改
		病毒库	不检查				
5	弱联动	杀毒引擎	不支持			<input type="checkbox"/>	查看 修改
		病毒库	检查	自适应顺延天数	7		NOD32 2.
7	弱联动	杀毒引擎	不支持			<input type="checkbox"/>	查看 修改
		病毒库	检查	自适应顺延天数	7		NOD32 2.

基本信息

杀毒软件名称

检查杀毒引擎版本

版本检查方式:

* 病毒库自适应顺延天数:

注意: 请输入病毒库自适应顺延天数, 它用来限制用户的病毒库最长可以不更新的天数

病毒扫描

认证后立即执行内存扫描

上报不能清除的病毒信息

启用全盘扫描

* 全盘扫描时间间隔:
 天

杀毒软件监视

全部监视

网页监视

文件监视

即时通信监视

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信息:

* 杀毒引擎及病毒库升级:

(. " ")

1.3.3

%

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

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, 192.168.1.23”, 配置成功后, 你可通过“系统中心”管理控制台查看SAM服务器的活动显示设备。

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

事件

安全事件

直接丢弃

记录日志

的安全事件

60 % 时直接丢弃

60 % 时只记录日志

192.168.6.193

以配置多个安全事件解析器, 它们之间使用逗号分隔, 如“192.168.1.23, 192.168.2.23”

网络攻击防治

开启网络攻击防治

记录非认证用户发起的安全

按可信度过滤对敏感资源的

* 可信度 <= 60 % 时直

* 可信度 <= 80 % 时只

按可信度过滤对非敏感资源

* 可信度 <=

* 可信度 <=

其他功能

* 第三方系统访

* 端点防护状态

* 软硬件配置信

访问端口: 9090 (默认为9090)

检测周期: 5 分钟 (默认为5分钟)

自报告周期: 5 分钟 (默认为100分钟)

分钟 (默认为60分钟)

* 访问控制策略同步周期: 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

修改 重置

1.4

PC

RG-SMP

1.4.1

[1.1](#)

1.4.2

%

“

>

”

“

”

端点防护策略模板版本信息 策略即编定 策略事件联动 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

启用锐捷客户端更新

必须安装的补丁类型：

全部类型

Service Pack 安全更新程序 自定义更新

安全更新程序 自定义更新

必须安装或补丁安全级别：

紧急 重要 次要

更新周期： 16

关键更新程序 Feature Pack

WUA下载地址： <http://support.microsoft.com/kb/927891/zh-cn>

更新过程采取安全措施

如果采取安全措施，用户在未完成补丁更新之前，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 禁用自动更新

允许自动更新立即安装： 启用

配置自动更新： 自动下载并计划安装

计划安装时间： 10:00

添加 重置 返回

注意：重置功能将重置所有选项卡中的信息。

&

“ ”

1.4.3

[1.3.4](#)

1.4.4

[1.3.5](#)

1.5

RG-SMP

PC

/

/

/

1.5.1

[1.1](#)

1.5.2

%

“

>

”

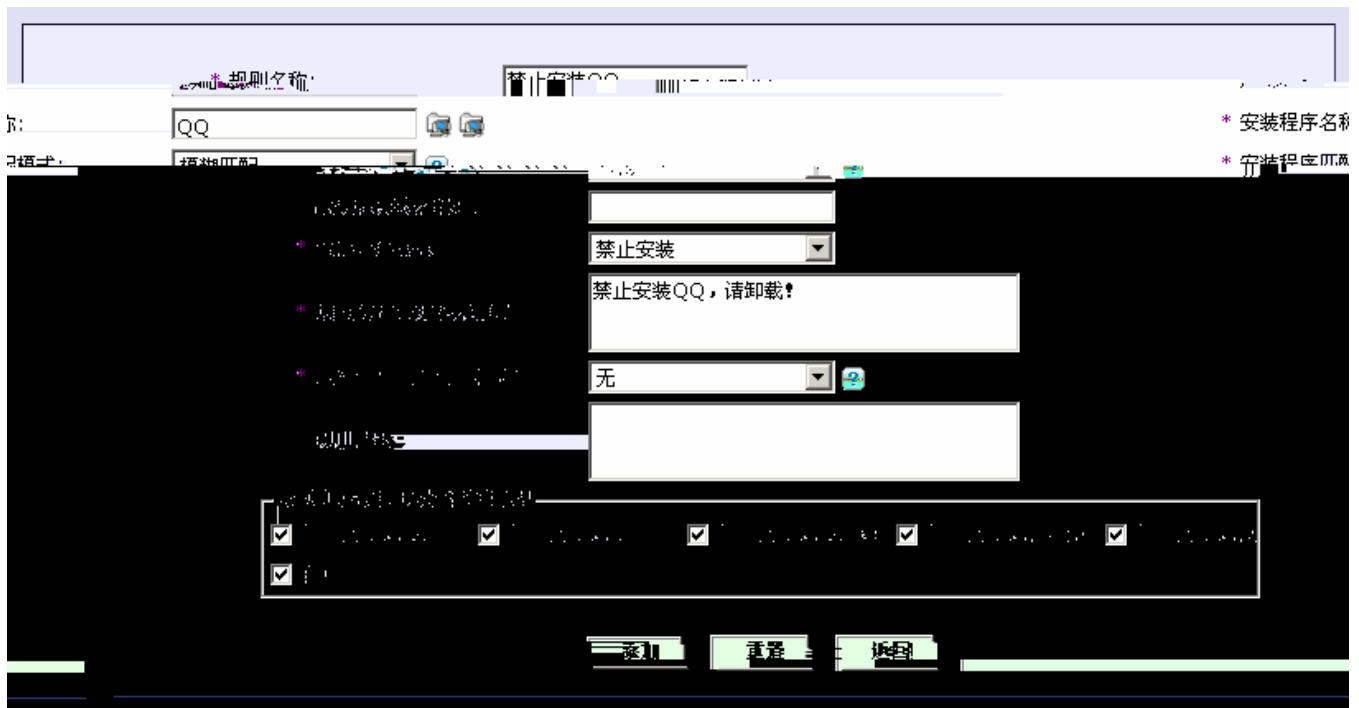
“

”

&

“

”



“

”

* 规则名称:

* 进程名称:

* 过滤模式:

* 端点防护失败提示信息:

* 端点防护失败修复模式:

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 Windows 7

全选

(. “ ”

* 规则名称:

* 注册表分支名称: 启动项快捷方式

* 注册表键名:

注册表键值类型:

键值表达式:

* 注册表键值:

* 注册表状态:

* 端点防护失败提示信息:

* 端点防护失败修复模式:

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 Windows 7

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; 当注册表状态为“禁止存在”, 将删除注册表键值。

). “ ”

规则组：锐捷测试_规则组

<input checked="" type="checkbox"/>	规则名称	规则类型	相应对象名称	相应对象状态	详细信息
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	强制停止Clipbook 服务	系统服务	ClipSrv	禁止启动	查看
<input checked="" type="checkbox"/>	禁止启动BQQ	进程	RTX	禁止运行	查看

(. “ ”

1.5.4

% “ > ” “ ”

规则组绑定

<input checked="" type="checkbox"/>	规则组名称	规则组类型	规则组描述	详细信息
<input checked="" type="checkbox"/>	锐捷测试_规则组	必备		查看

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
RG-SMP
U

PCMCIA

PC

1.6.1

[1.1](#)

1.6.2

% “ >

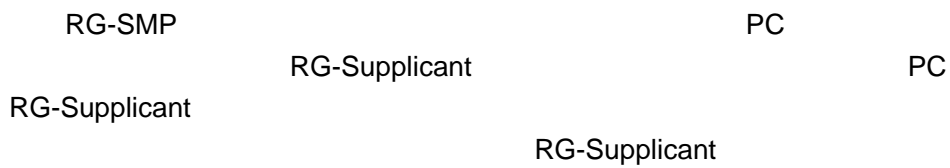


& “ ”

1.6.3

[1.3.5](#)

1.7



1.7.1

[1.1](#)

1.7.2

%

“

>

”

“

”

1.8.2

RG-SEP

%

“ ”

“ ”

RG-SEP

接入用户控制

定期检测用户在线状态

* SAM服务器IP:

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, 192.168.1.23, 192.168.1.23”。配置成功后, 你可通过“系统日志”对话框以该地址来查看SAM服务器的启动显示页。

客户端配置文件

* 配置文件更新周期: 分钟 (默认为60分钟)

* 配置文件更新服务器:

配置文件更新服务器是指存放给终端安全认证客户端初始化配置的FTP服务器地址。地址的根目录指向SMP安装在服务器的配置文件。

网络攻击防治

开启网络攻击防治

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 <= % 时直接丢弃

* 可信度 <= % 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 <= % 时直接丢弃

* 可信度 <= % 时只记录日志

* 安全策略解释器IP:

注意: 可以配置多个安全策略解释器IP, IP之间使用逗号分隔, 如“192.168.6.193, 192.168.6.23”。

其他功能

* 第三方系统访问端口: (默认为9090)

* 端点防护状态检测周期: 分钟 (默认为5分钟)

* 软硬件配置信息报告周期: 分钟 (默认为120分钟)

漏洞检测策略信息更新周期: 分钟 (默认为120分钟)

* 修复服务器:

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。

&

“ ”

1.8.3

%

“ ”

启用ARP欺骗免疫功能

共10条记录 每页20条 第1页/共1页 GO [首页] [上一页] [下一页] [尾页]

网关IP ↑	网关MAC ↑	网关名称 ↑	网关类型 ↑	应用模式	支持防ARP欺骗	开启防ARP欺骗	操作
接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.150	00D0F82233AD	S3250	S3250-48
接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.156	00D0F8223389	xsf	S2652G
接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.161	001AA918E617	Ruijie	S2628G
接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.163	00D0F8EDCD5A	xsf	其它类型
S2652G	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.169	00D0F82233AF	my switch
S3750-24	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.172	00D0F8C7A4E1	Ruijie
S8606	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.199	00D0F812341B	Ruijie
S2150G	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.254	00D0F8BF9EB4	apache
S2126G	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.90	00D0F8BC9556	GSN

& “ ARP ”

启用ARP欺骗免疫功能

共10条记录 每页20条 第1页/共1页 GO [首页] [上一页] [下一页] [尾页]

网关IP ↑	网关MAC ↑	网关名称 ↑	网关类型 ↑	应用模式	支持防ARP欺骗	开启防ARP欺骗	操作
192.168.203.1	00D0F8BC9511			网关	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	查看
192.168.203.150	00D0F82233AD	S3250	S3250-48	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看
192.168.203.156	00D0F8223389	xsf	S2652G	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看
192.168.203.161	001AA918E617	Ruijie	S2628G	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看
192.168.203.163	00D0F8EDCD5A	xsf	其它类型	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看
192.168.203.169	00D0F82233AF	my switch	S2652G	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看
192.168.203.172	00D0F8C7A4E1	Ruijie	S3750-24	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看
192.168.203.199	00D0F812341B	Ruijie	S8606	接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看
192.168.203.254	00D0F8BF9EB4			接入与网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看
192.168.203.90	00D0F8BC9556	GSN	S2126G	接入与网关	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	查看

说明

“ ARP ”

ARP

“ ARP ”

ARP

ARP

2

Red-Giant Security Management Platform (SMP)

SMP

- ' _____
- ' _____
- ' _____
- ' _____
- ' _____
- ' _____
- ' _____
- ' _____
- ' _____
- ' _____
- ' _____
- ' _____
- ' _____

2.1

SMP

- ' _____
- ' _____
- ' _____
- ' _____
- ' _____

2.1.1

SMP


±	-----	SMP	supervisor
	ruijiesmp		
±	-----	SMP	log
	111111111		
±	-----	SMP	admin
		SMP	111111111

2.1.2

SMP

±	supervisor	ruijiesmp
±	log	111111111
±	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:

创建时间 (结束):

共3条记录 每页20条 第1页/共1页 GO

[\[首页\]](#) [\[上一页\]](#) [\[下一页\]](#) [\[尾页\]](#)

<input type="checkbox"/>	用户名 ↑	所属用户组 ↑	创建时间 ↑	操作
<input type="checkbox"/>	admin	系统管理员	2009-07-17 11:29:53	查看 修改
<input type="checkbox"/>	log	日志管理员	2009-07-17 11:29:53	查看 修改
<input checked="" type="checkbox"/>	supervisor	超级管理员	2009-07-17 11:29:53	查看 修改

&

“ ”

“ ”

“

,

“ ”

“ ”

(

Ø

“ ”

“ ”

“

Ø

“ ”

“ ”

Ø

Ø

“ ”

“ ”

“

 说明

2.1.5.2

%

“ ”

“ ”

“

”

* 用户名: ?

* 所属用户组: ▼

* 密码: ?

* 密码确认:

真实姓名:

Email地址:

电话号码:

& “ ”

' " ” “ ” “ ”

(“ ”

). “ ” “ ”

说明

,

“**”

SUPERVISOR() system()

* 用户名: ?

* 所属用户组: ▼

密码: ?

密码确认:

真实姓名:

Email地址:

电话号码:

& " "

' " " " " "

(" "

). " " " "

说明

'

' 9 20

' supervisor

2.1.5.4

" "

" "

2.2

SMP

'

' _____

' _____

' _____

' _____
' _____
' _____
' _____

2.2.1

± _____, RG-SAM
, _____,

±

±

1

2

1

±

1

2

1

2.2.2

SMP

SAM

SMP

2.2.2.1

%

“

”

“

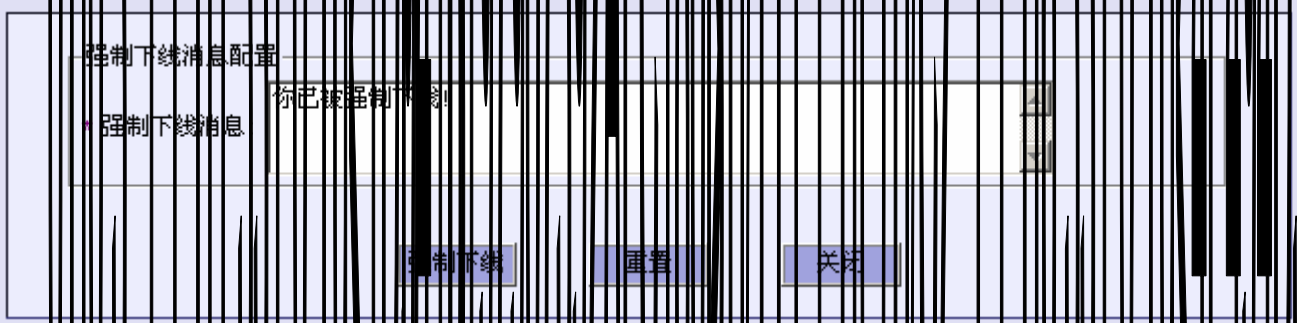
”

“

”

2.2.2.3

%



&

'

(

 说明


2.2.2.4

“

”

“

”

 说明

说明

2.2.2.6

% “ ” “ ” “ ”

The screenshot shows a configuration dialog box with a light blue background. It contains the following elements:

- 消息内容:** A large text input field with vertical scrollbars.
- 修复程序类型:** A dropdown menu currently set to "下载补丁" (Download Patch), with a blue question mark icon to its right.
- 修复程序URL:** A text input field currently containing "无" (None), with a blue question mark icon to its right.
- * 修复程序URL:** A label positioned to the left of the URL input field.
- 验证URL:** A button located to the right of the URL input field.
- 下发:** A button at the bottom left.
- 重置:** A button at the bottom center.
- 关闭:** A button at the bottom right.

& “ ”

' “

(“

). “

URL

URL

2.2.3

SMP

2.2.3.1

%

用户组名称: 用户组描述:
 安全策略模板: 用户访问权限:

共4条记录 每页20条 第1页/共1页 GO [首页] [上一页] [下一页] [尾页]

<input type="checkbox"/>	用户组名称 ↑	安全策略模板	用户访问权限	用户组描述	操作
<input type="checkbox"/>	领导组	default	默认用户访问权限		修改
<input type="checkbox"/>	老师组	default	默认用户访问权限		修改
<input type="checkbox"/>	学生组	default	默认用户访问权限		修改
<input type="checkbox"/>	默认用户组	default	默认用户访问权限	系统默认的用户组!	修改

&

'

(

Ø

Ø

Ø

Ø

Ø

说明

2.2.3.2

% “ ” “ ” “ ”

* 用户组名称:

* 安全策略模板:

* 用户访问权限:

用户组描述:

1. 如果用户所在的交换机绑定了安全策略模板, 那么这里绑定的安全策略模板将不生效.
 2. 如果用户或用户所在的交换机绑定了用户访问权限, 那么这里绑定的用户访问权限将不生效.

& “ ”

! “ ” “ ” “ ”

(“ ”

). “ ” “ ”

说明

! “*” 32 16

2.2.3.3

% “ ” “ ” “ ”

* 用户组名称:

* 安全策略模板:

* 用户访问权限:

用户组描述:

1. 如果用户所在的交换机绑定了安全策略模板, 那么这里绑定的安全策略模板将不生效。
2. 如果用户或用户所在的交换机绑定了用户访问权限, 那么这里绑定的用户访问权限将不生效。
3. 如果用户组正在被在线用户使用, 您的修改将在用户下次认证时生效。

& “ ”

‘ “ ” “ ” “ ”

(“ ”

). “ ” “ ”

说明

2.2.3.4

“ ” “ ”

说明

2.2.4

SMP

2.2.4.1

%

“ ” “ ” “ ”

用户访问权限名称: 控制方式:

共1条记录 每页20条 第1页/共1页 [GO](#) [\[首页\]](#) [\[上一页\]](#) [\[下一页\]](#) [\[尾页\]](#)

<input type="checkbox"/>	用户访问权限名称 ↑	控制方式 ↑	操作
<input type="checkbox"/>	默认用户访问权限	不控制	查看 修改

&

“ ” “ ” “ ”

'

“ ” “ ”

(

∅

“ ” “ ” “ ”

∅

“ ” “ ”

∅

∅

“ ” “ ” “ ”

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

<input checked="" type="checkbox"/>	上网权限模板名称	描述	操作
<input checked="" type="checkbox"/>	允许访问日志系统		查看
<input checked="" type="checkbox"/>	禁止访问所有网络资源		查看

& “ ”

“ ” “ ” “ ”

(“ ”

) “ ” “ ”

说明

“**” 32 16

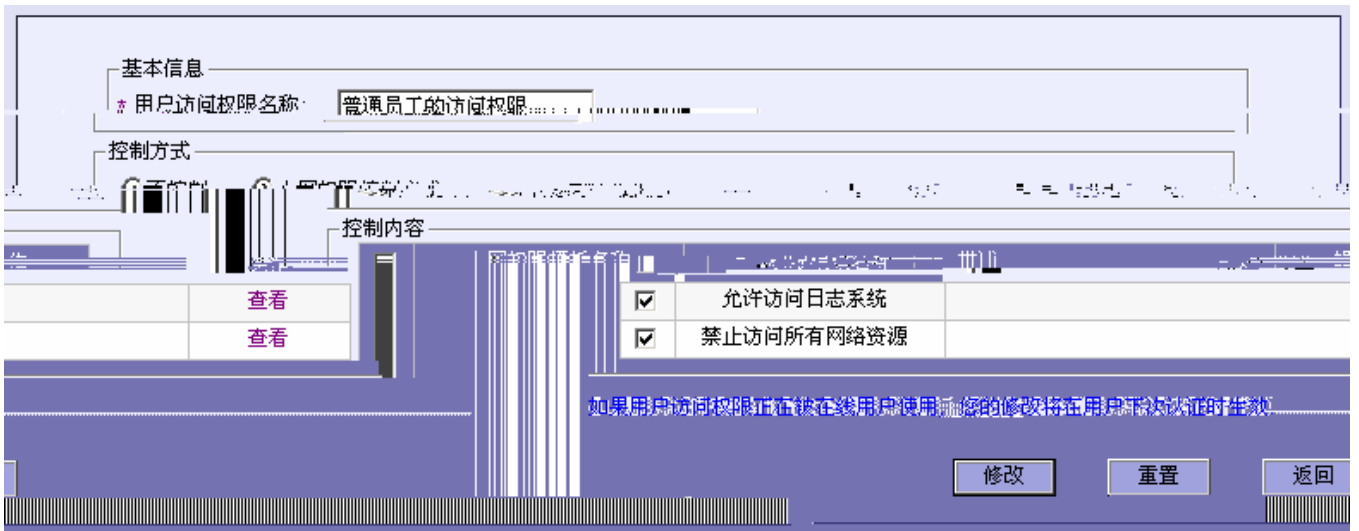
“ ”

“ ”

“ ”

2.2.4.3

% “ ” “ ” “ ”



& “ ”

‘ “ ” “ ” “ ”

(“ ”

). “ ” “ ”

 说明

2.2.4.4

“ ” “ ”

 说明

2.2.5

SMP

2.2.5.1

% “ ” “ ” “ ”

安全策略模板名称: 安全策略模板描述: [高级查询](#)

共1条记录 每页20条 第1页/共1页 [GO](#) [\[首页\]](#) [\[上一页\]](#) [\[下一页\]](#) [\[尾页\]](#)

<input type="checkbox"/>	安全策略模板名称	安全策略模板描述	操作
<input type="checkbox"/>	安全策略模板名称	安全策略模板描述	删除 修改

& “ ” “ ” “ ” “ ”

! “ ” “ ” “ ” “ ”

(“ ” “ ” “ ” “ ”

).

∅ “ ” “ ” “ ” “ ” “ ”

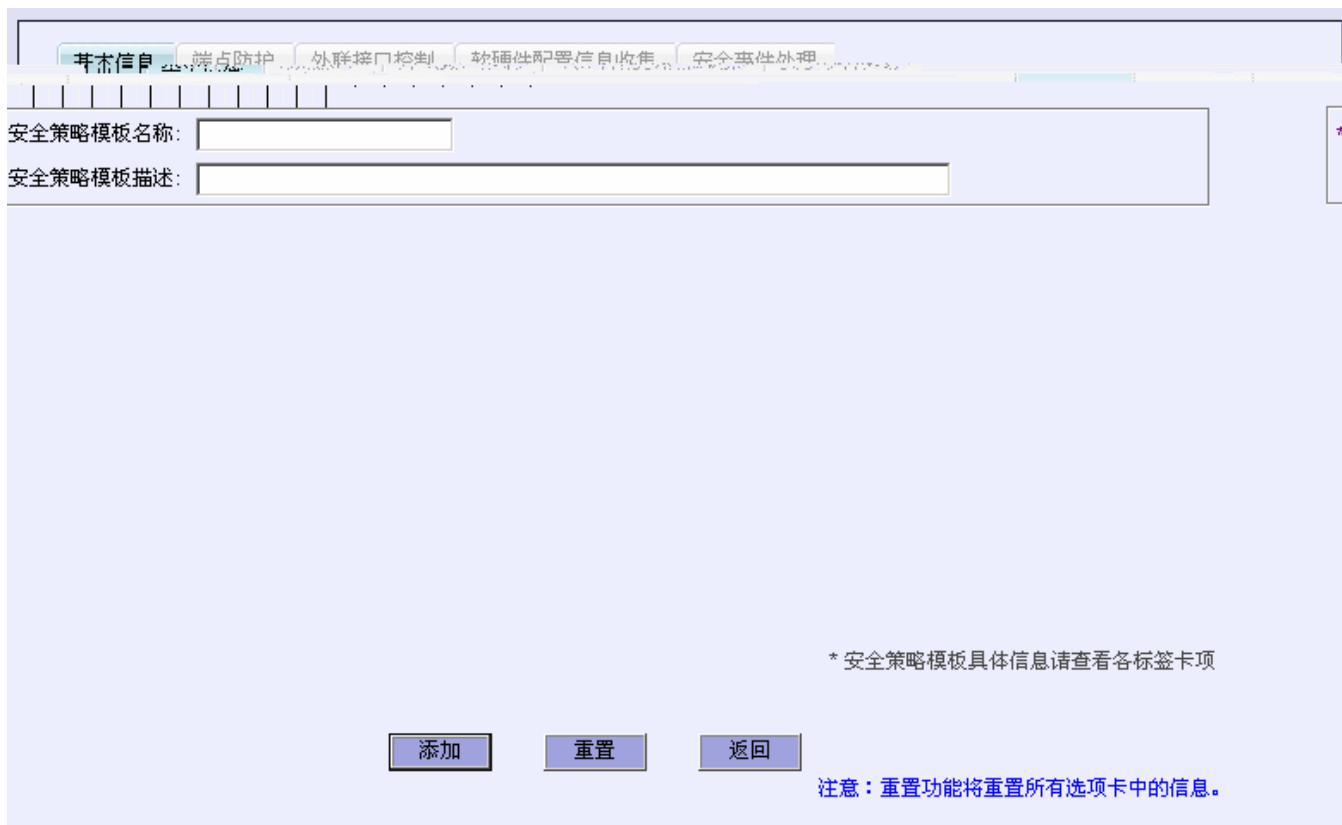
∅ “ ” “ ” “ ” “ ” “ ”

∅

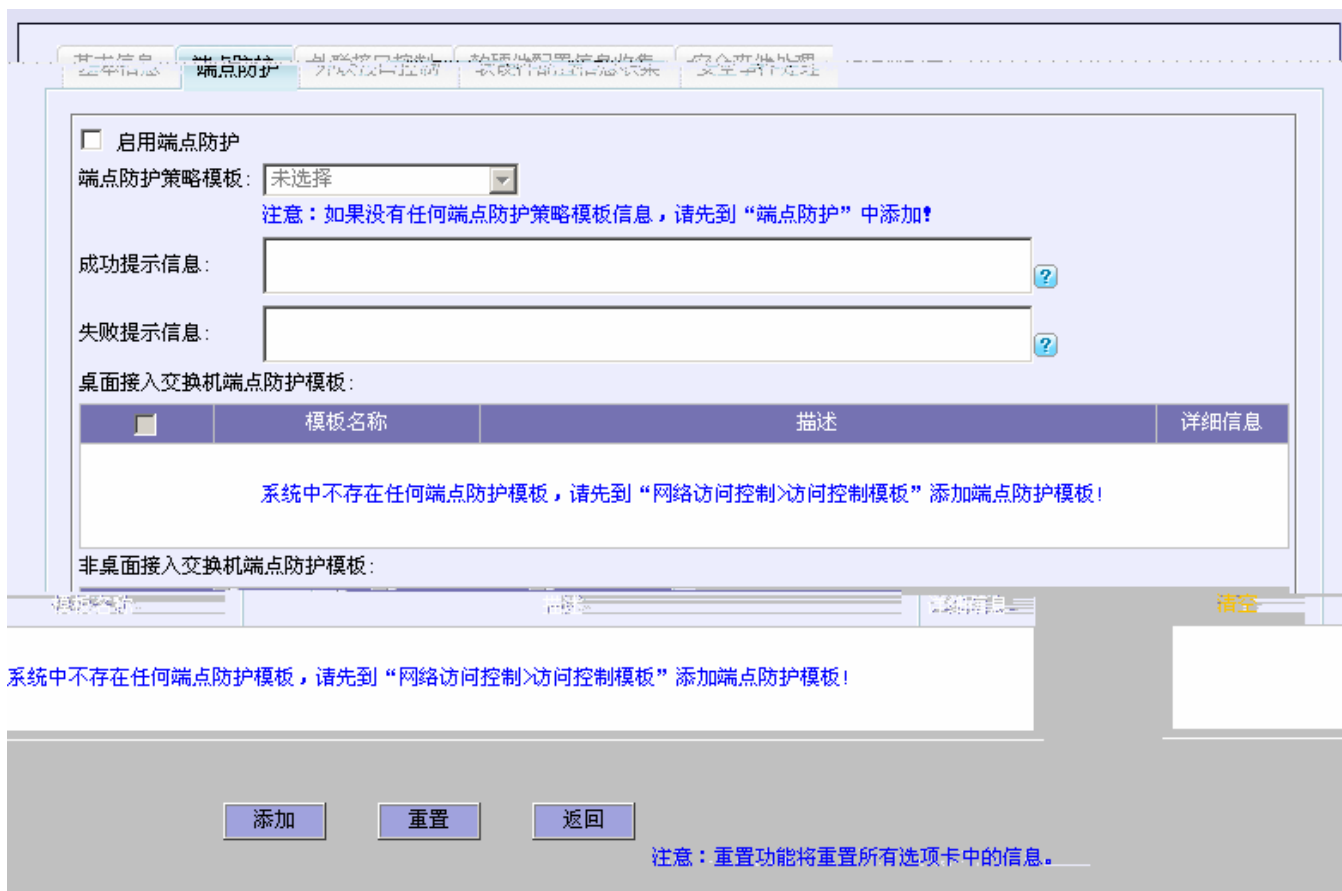
∅ “ ” “ ” “ ” “ ” “ ”

2.2.5.2

% “ ” “ ” “ ” “ ” “ ”



& “ ”



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

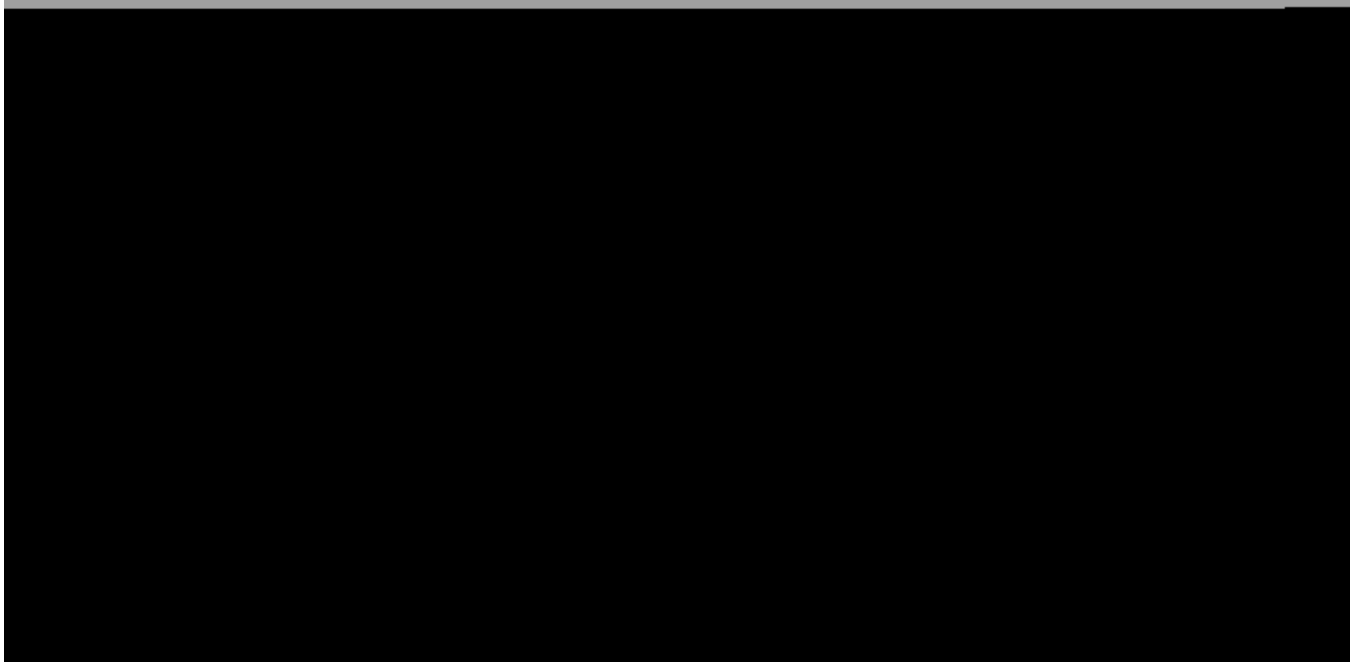
返回

注意：重置功能将重置所有选项卡中的信息。

(. “ ”

措施

应用安全



* “ ” “ ” “ ”

+ “ ”

“ ” “ ”

说明

“**”

32

16

“ ”

“ ”

“

”

“ ” “ ”

,

2.2.5.4

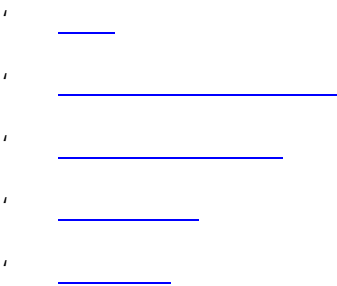
“ ” “ ”

说明

,

2.3

SMP



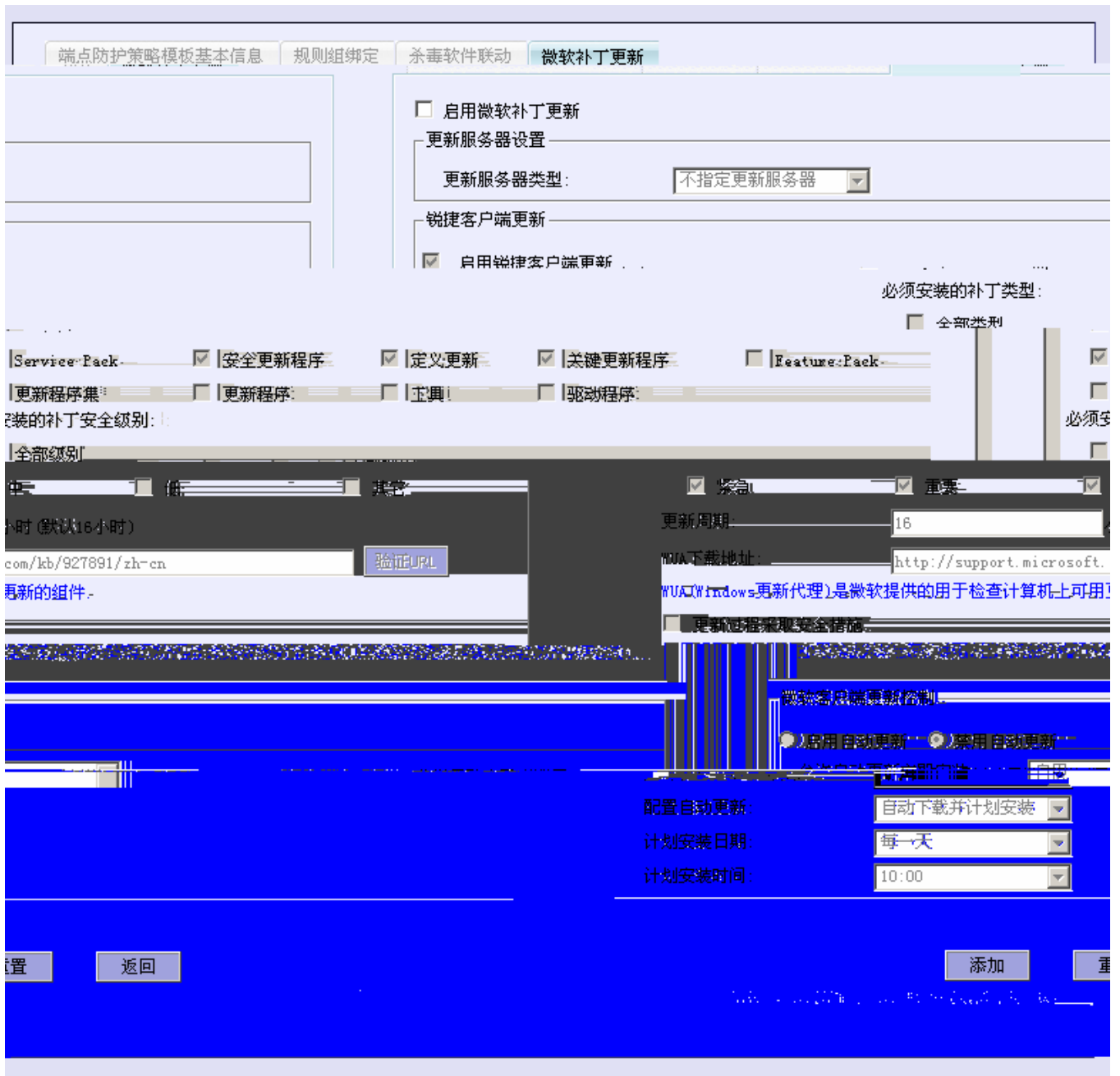
2.3.1

±

“ 2008 ”

±

(.



“ ”

).

“ ”

“

”

“

”

*

“ ”

+

“ ”

“

”

说明

“*”

32

16

2.3.2.3

%

“

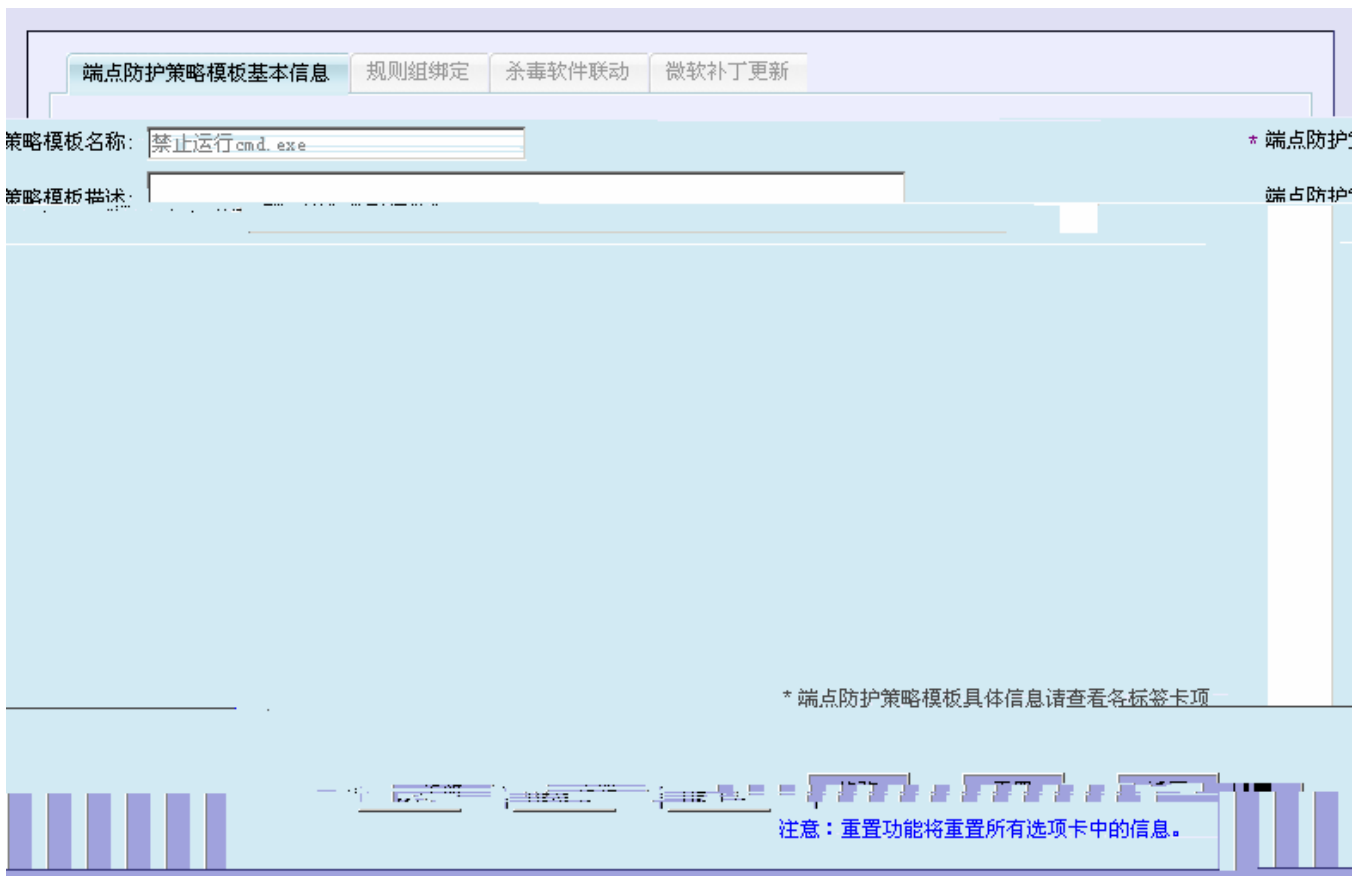
”

“

”

“

”



&

“

”

‘

“

”

“

”

“

”

(

“

”

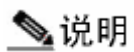
)

“

”


“

”



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	自适应顺延天数	7	<input type="checkbox"/>	查看 修改
		病毒库	检查				
江民杀毒软件KV2007	弱联动	杀毒引擎	不检查	自适应顺延天数	7	<input type="checkbox"/>	查看 修改
		病毒库	检查				
卡巴斯基反病毒软件6.0	弱联动	杀毒引擎	不支持	自适应顺延天数	7	<input type="checkbox"/>	查看 修改
		病毒库	检查				
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	自适应顺延天数	7	<input type="checkbox"/>	查看 修改
		病毒库	检查				
		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
<input type="checkbox"/>	查看 修改	Symantec AntiVirus企业版 8	弱联动	杀毒引擎	不检查		
				病毒库	检查	自适应顺延天数	7
<input type="checkbox"/>	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
<input type="checkbox"/>	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
				杀毒引擎	检查	自适应顺延天数	7
V10.0	弱联动	杀毒引擎	不检查				McAfee VirusScan
		病毒库	不检查			<input type="checkbox"/>	查看 修改
enterprise	弱联动	杀毒引擎	不检查				McAfee VirusScan En
		病毒库	不检查			<input type="checkbox"/>	查看 修改
				杀毒引擎	检查	自适应顺延天数	7
				病毒库	检查	自适应顺延天数	7
自适应顺延天数	7					<input type="checkbox"/>	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					<input type="checkbox"/>	查看 修改
				NOD32 2.7	弱联动	杀毒引擎	不支持
						病毒库	检查
				趋势科技 PC cillin V2005 网络安	弱联动	杀毒引擎	不检查
						病毒库	不检查
				趋势科技 PC cillin V2007 网络安	弱联动	杀毒引擎	不检查
				全版		病毒库	不检查
				奇虎360安全卫士	弱联动	杀毒引擎	不支持
						病毒库	检查
自适应顺延天数	7					<input type="checkbox"/>	查看 修改
自适应顺延天数	7					<input type="checkbox"/>	查看 修改
自适应顺延天数	7					<input type="checkbox"/>	查看 修改
自适应顺延天数	7					<input type="checkbox"/>	查看 修改
自适应顺延天数	7					<input type="checkbox"/>	查看 修改
自适应顺延天数	7					<input type="checkbox"/>	查看 修改
自适应顺延天数	7					<input type="checkbox"/>	查看 修改
弱联动		杀毒引擎	不检查				
		病毒库	检查	自适应顺延天数	7	<input type="checkbox"/>	查看 修改
弱联动		杀毒引擎	不检查				
		病毒库	检查	自适应顺延天数	7	<input type="checkbox"/>	查看 修改
v1	弱联动	杀毒引擎	不检查				
		病毒库	不检查			<input type="checkbox"/>	查看 修改
							瑞星杀毒软件2007(企业版)
							瑞星杀毒软件网络版2008(企业版)
							Bitdefender Internet Security
							0

&

,

Ø

“ ”

“

”

“

”

2.3.3.2

%

“

”

“

”

“

”



“ ”

(“ ” “ ” “ ”

) “ ”

* “ ” “ ”

说明

/

/ “ ” “ ”

”

“ ”

2.3.4

SMP

2.3.4.1

% “ ” “ ” “ ” “ ” “ ”

“ ”

规则组名称: 规则组类型:

端点防护策略模板名称: 规则名称:

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]

<input type="checkbox"/>	规则组名称 ↑	规则组描述	规则组类型 ↑	操作
<input type="checkbox"/>	禁止运行cmd.exe		必备	查看 修改 修改绑定

& " " " "

' " " " "

(.

Ø " " " "


Ø " " " "

Ø

Ø " " " " "

Ø " " " " "

Ø " " " " "

 说明

2.3.4.2

% " " " " " "

* 规则组名称:

* 规则组类型:

* 端点防护失败提示信息:

* 端点防护失败修复模式: ?

规则组描述:

& " "

' " " " "

(" " " " "

规则组: fewafewfwa

<input type="checkbox"/>	规则名称	规则类型	相应对象名称	相应对象状态	详细信息
<input type="checkbox"/>	禁止运行 cmd.exe	进程	cmd.exe	禁止运行	查看

) " "

* " " " "

+ " " " " " "

说明

“*” 64 32

“ ” “ ” “ ”

“ ”

2.3.4.3

% “ ” “ ” “ ”

* 规则组名称:	<input type="text" value="禁止运行cmd.exe"/>
* 规则组类型:	必备
规则组描述:	<input type="text"/>
<input type="button" value="修改"/> <input type="button" value="重置"/> <input type="button" value="返回"/>	

* 规则组名称:	<input type="text" value="可以使用qq"/>
* 规则组类型:	可选
<input type="text"/>	
<input type="text"/>	
<input type="button" value="重置"/> <input type="button" value="返回"/>	
	* 端点防护失败提示信息: <input type="text" value="可以使用qq"/>
	* 端点防护失败修复模式: <input type="text" value="无"/>
	规则组描述: <input type="text"/>
	<input type="button" value="修改"/>

& “ ”
, “ ” “ ” “ ” “ ”
(“ ”
) “ ” “ ”

 说明

2.3.4.4

“ ” “ ”

说明

2.3.4.5

% “ ” “ ” “ ”

规则组：可以使用QQ

<input type="checkbox"/>	规则名称	规则类型	相应对象名称	相应对象状态	详细信息
<input type="checkbox"/>	禁止运行cmd.exe	进程	cmd.exe	禁止运行	查看

& “ ”
' “ ” “ ” “ ”
(“ ”
) “ ” “ ”

2.3.5

SMP

2.3.5.1

% “ ” “ ” “ ” “ ” “ ”

* 规则名称:

* 安装程序名称:

* 安装程序匹配模式: 模糊匹配

安装程序版本号:

* 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 Windows Vista Windows 7

全选

& “ ”

! “ ” “ ” “ ”

(“ ”

) “ ” “ ”

说明

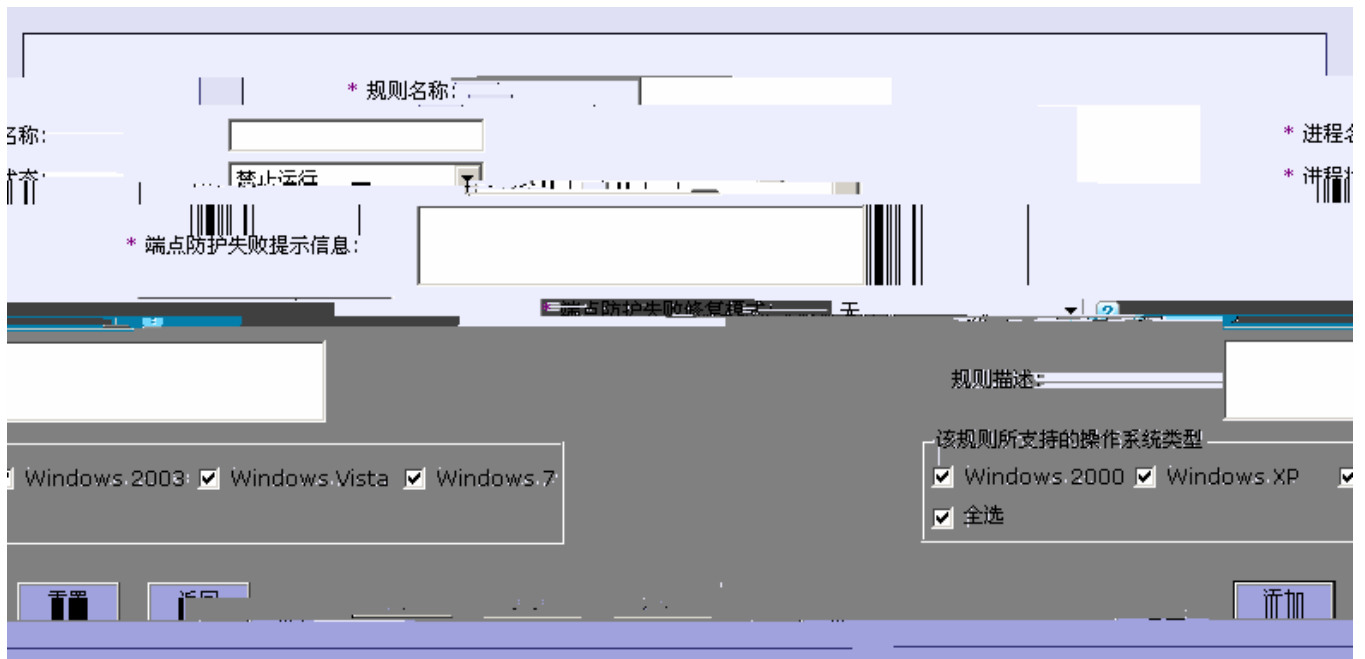
“*” 128 64

“ ” “ ” “ ”

“ ”

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:

注册表键值类型:

键值表达式:

注册表键值:

* 注册表状态:

* 端点防护失败提示信息:

* 端点防护失败修复模式: ?

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 Windows 7

全选


注: 勾选全部操作系统类型时, 规则将适用于所有支持的操作系统。勾选部分操作系统类型时, 规则将只适用于勾选的操作系统。

& “ ”

! “ ” “ ”

(“ ”

). “ ” “ ”

 说明

“*”	128	64
“ ”		
“ ”		
“ ”		
“ ”		
“ ”		

2.3.5.5

% “ ” “ ” “ ”

* 规则名称:

* 系统服务名称:

* 系统服务状态: 禁止启动

* 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 Windows 7

全选

添加 重置 返回

& “ ”

! “ ” “ ” “ ” “ ”

(“ ”

) “ ” “ ”

说明

“**”

128

64


2.3.5.6

% “ ” “ ” “ ”
& “ ”
, “ ” “ ” “ ”
(, “ ”
) “ ” “ ”

 说明

2.3.5.7

“ ” “ ”

 说明

2.3.5.8

% “ ” “ ” “ ” “ ” “ ”

规则文件 (*.dat): 浏览...

注意: 规则文件最大不能超过10MB。

规则导入

重置

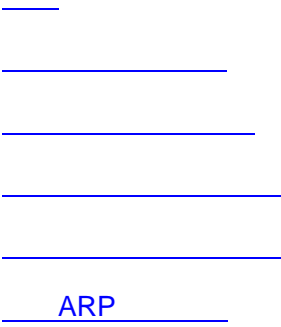
返回

& “ ...”

.dat

2.4

SMP



2.4.1

±

±

SMP

±

±

±

ARP

ARP

2.4.2

SMP

2.4.2.1

%

“

”

“

”

“

”

敏感资源描述:

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]

<input type="checkbox"/>	敏感资源IP ↑	子网掩码	敏感资源名称 ↑	敏感资源描述	操作
<input type="checkbox"/>	192.168.203.1	255.255.255.255	核心网关	公司的核心网关	查看 修改

& " " " " " "

' " " " " "

(

∅ " " " " "

∅ " " " " "

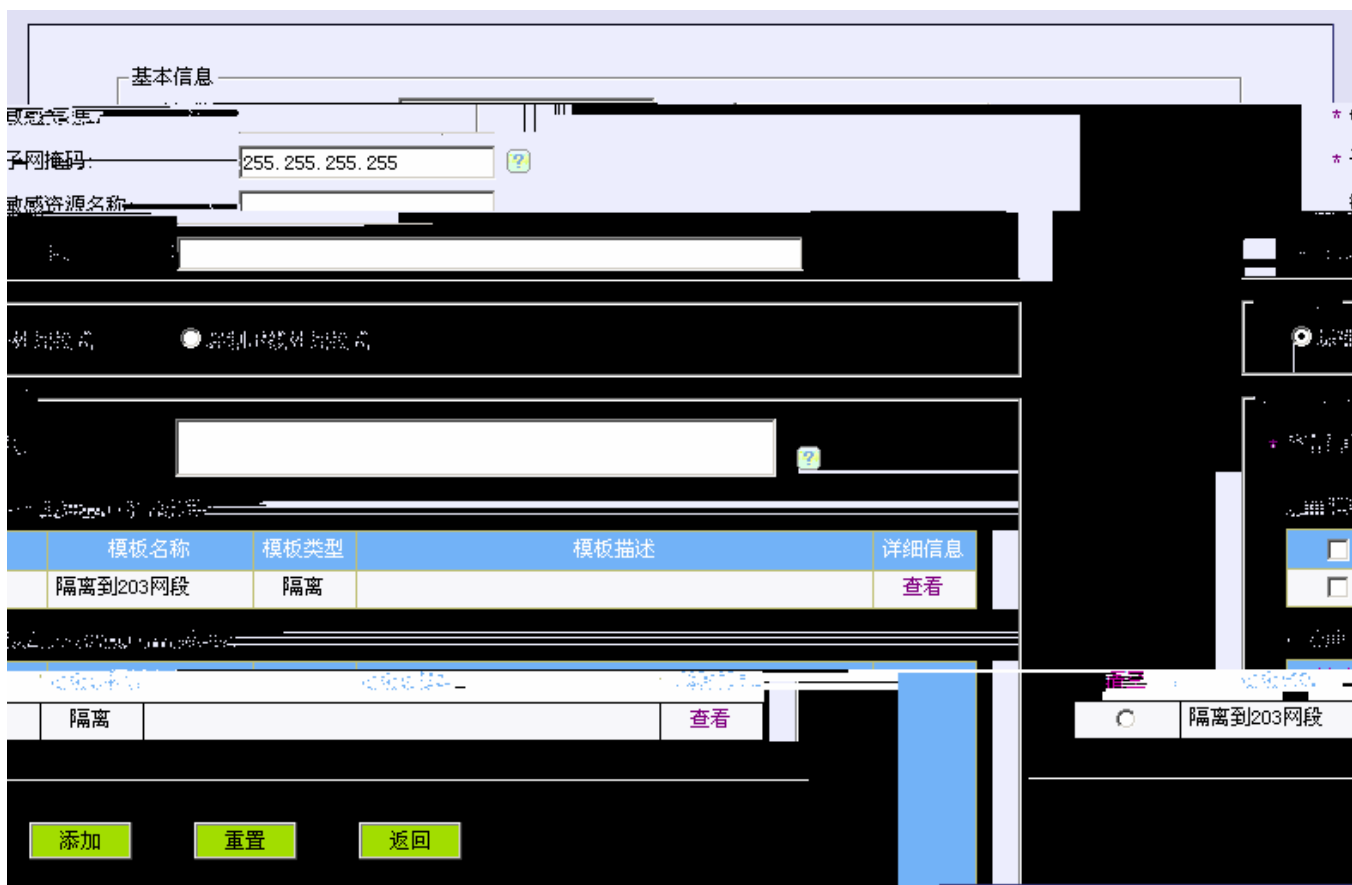
∅

∅ " " " " "

 说明

2.4.2.2

% " " " " " "



&

' " " " " "

(" "

) " " " "

说明

“**”

‘

‘

‘

“ ”

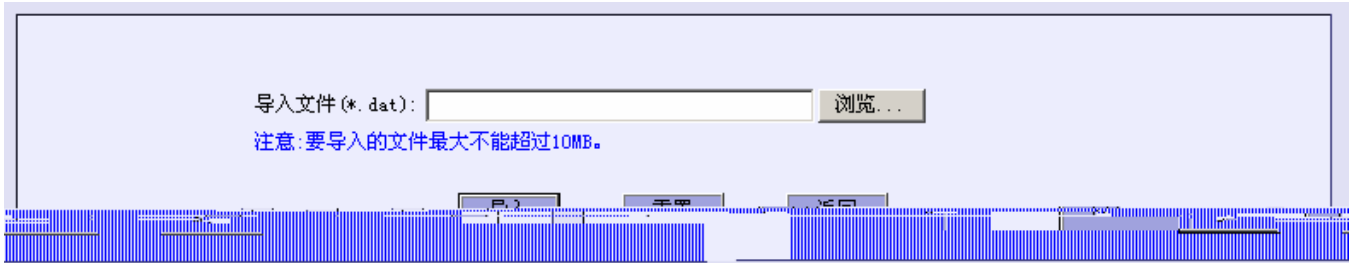
“ ”

2.4.2.3

%

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。		
“熊猫烧香”病毒是于2004年11月26日由网络安全专家周冠微发现的。该病毒以“熊猫烧香”为名称，其图标为一只正在烧香的熊猫。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: +请把杀毒软件更新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

安全措施: 应用安全事件处理模板

应用安全事件处理模板

添加安全事件处理模板

“熊猫烧香”是用delphi编写的病毒,作为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。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标,诱使计算机用户运行。

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

“ ”

“ ” “ ”

2.4.3.7

“ ” “ ”

 说明

2.4.5.1

%

”

安全事件处理模板名称: 模板描述:

<input type="checkbox"/>	安全事件处理模板名称 ↑	处理模式	模板描述	操作
<input type="checkbox"/>	普通级别处理模板	标准处理模式	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!	查看 修改
<input type="checkbox"/>	严重级别处理模板	标准处理模式	攻击频率处理模式默认模板，用于严重级别安全事件的处理!	查看 修改
<input type="checkbox"/>			攻击频率处理模式默认模板，用于灾难性级别安全事件	查看 修改

&

“

”

,

“

”

“

”

(

∅

“

”

“

”

“

”

2.4.5.2

% “ ” “ ” “ ”

基本信息

* 安全事件处理模板名称:

安全事件处理模板描述:

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

* 无 (只对处理对象进行日志记录, 不进行其它任何处理!)

& “ ”

“ ” “ ” “ ” “ ”

(“ ”

) “ ” “ ”

说明

“*” 64 32

“ ” “ ” “ ” “ ”

2.4.5.3

% “ ” “ ” “ ” “ ”

基本信息

* 安全事件处理模板名称:

安全事件处理模板描述:

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: ?

桌面接入交换机访问控制模板:

<input type="checkbox"/>	模板名称	模板类型	模板描述	详细信息
<input type="checkbox"/>	禁止访问HTTP服务	阻断	禁止用户访问Http服务	查看
<input type="checkbox"/>	禁止访问FTP服务	阻断	禁止用户访问FTP服务	查看
<input type="checkbox"/>	禁止访问TELNET服务	阻断	禁止用户访问TELNET服务	查看
<input type="checkbox"/>	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
<input type="radio"/>	隔离到203网段	隔离		查看

& “ ”

‘ ’ “ ” “ ” “ ”

”


(“ ”

) “ ” “ ”

说明

2.4.5.4

“ ” “ ”

 说明

2.4.6 ARP

% “ ” “ARP” “ ARP ”

启用ARP欺骗免疫功能

共15条记录 每页1条 第1页 (共15页) [首页] [上一面] [下一面] [尾页]


开启防ARP欺骗	操作	网关IP ↑	网关MAC ↑	网关名称 ↑	网关类型 ↑	应用模式	支持防ARP欺骗
<input type="checkbox"/>	查看	192.168.203.149	001AA90F9163	zqd-test	S2628G	接入与网关	<input checked="" type="checkbox"/>

& “ ”

' “ ARP ” ARP

(“ ARP ” ARP

) “ ARP ” ARP

 说明

' ARP

' “ > ” ARP ARP

2.5

SMP

' _____
' _____
' _____
' _____

'

2.5.1

±

±

±

±

HTTP FTP

策略编号:

用户IP:

目的IP:

用户名:

交换机IP:

[高级查询](#)

共1条记录 每页20条 第1页/共1页 [GO](#)

[\[首页\]](#) [\[上一页\]](#) [\[下一页\]](#) [\[尾页\]](#)

<input type="checkbox"/>	策略编号	策略类型	交换机IP	用户IP	目的IP	用户名	是否安装	操作
<input type="checkbox"/>	10396	阻断	192.168.203.90			1.1.1.3		是

& " " " " " "

' " " " " "

(.


Ø " " " " "

Ø " " " " "

Ø " " " " "

Ø " " " " "

Ø " " " " "

 说明

2.5.2.2

% " " " " " "

2.5.3.2

% “ ” “ ” “ ”

* 访问控制模板名称:	<input type="text"/>
访问控制模板描述:	<input type="text"/>
* 目的IP:	<input type="text"/>
* 子网掩码:	<input type="text" value="255.255.255.255"/>
目的MAC:	<input type="text"/>
目的端口:	<input type="text"/>
协议选择:	<input type="text" value="不选择"/>
<input type="button" value="添加"/> <input type="button" value="重置"/> <input type="button" value="返回"/>	

& “ ”

! “ ” “ ” “ ”

(“ ”

) “ ” “ ”

* 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:

策略生存方式:

& “ ”

! “ ” “ ” “ ”

(“ ”

) “ ” “ ”

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:


策略生存方式:

& “ ”

' “ ” “ ” “ ”

(. “ ”

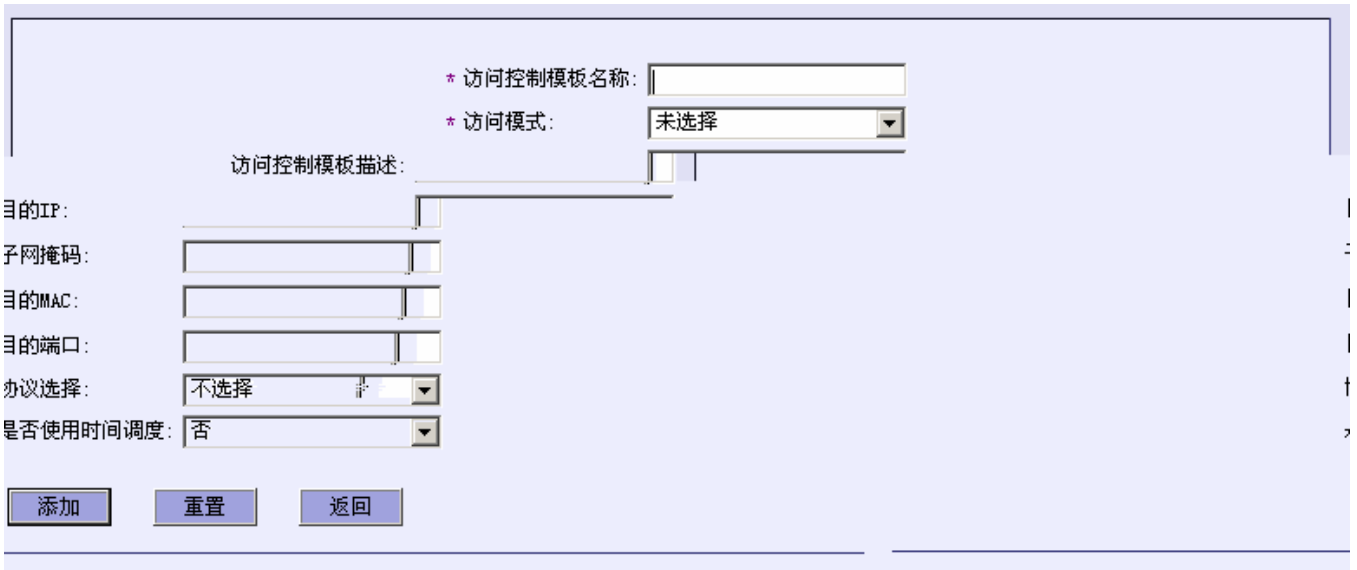
). “ ” “ ”

 说明

“*” 32 16

2.5.3.5

% “ ” “ ” “ ”




& “ ”

' “ ” “ ” “ ” “ ”

”

(. “ ”

). “ ” “ ”

 说明

“*”

32

16

“

“ ” “ ”

“ ”

2.5.3.6

% “ ” “ ” “ ”

& “ ”

“ ” “ ” “ ”

(. “ ”

). “ ” “ ”

说明

“

”

“ ” “ ” “ ” “ ”

“ ” “ ” “ ” “ ”

“ ”

2.5.3.7

“ ” “ ”

说明

“

2.5.4

SMP

2.5.4.1

%

”

“

”

“

”

“

访问控制模板组名称:

访问控制模板组描述:

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]

<input type="checkbox"/>	访问控制模板组名称 ↑	访问控制模板组描述	操作
<input type="checkbox"/>	禁止访问网络		查看 修改

&

“

”

“

”

“

”

,

“

”

“

”

”

(

∅

“

”

“

”

“

”

∅

“

”

“

”

∅

∅

“

”

“

”

“

”

 说明

2.5.4.2

% “ ” “ ” “ ”

基本信息

* 访问控制模板组名称:

访问控制模板组描述:

访问控制模板

<input type="checkbox"/>	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
<input type="checkbox"/>	隔离到203网段	隔离		查看
<input type="checkbox"/>	禁止访问TELNET服务	阻断	禁止用户访问TELNET服务	查看
<input type="checkbox"/>	访问FTP服务	阻断	禁止用户访问FTP服务	查看
<input type="checkbox"/>	访问HTTP服务	阻断	禁止用户访问Http服务	查看

禁止 禁止

& “ ”

' “ ”

(. “ ”

). “ ” “ ”

说明

“*”

32

16

2.5.4.3

% “ ” “ ” “ ”

基本信息

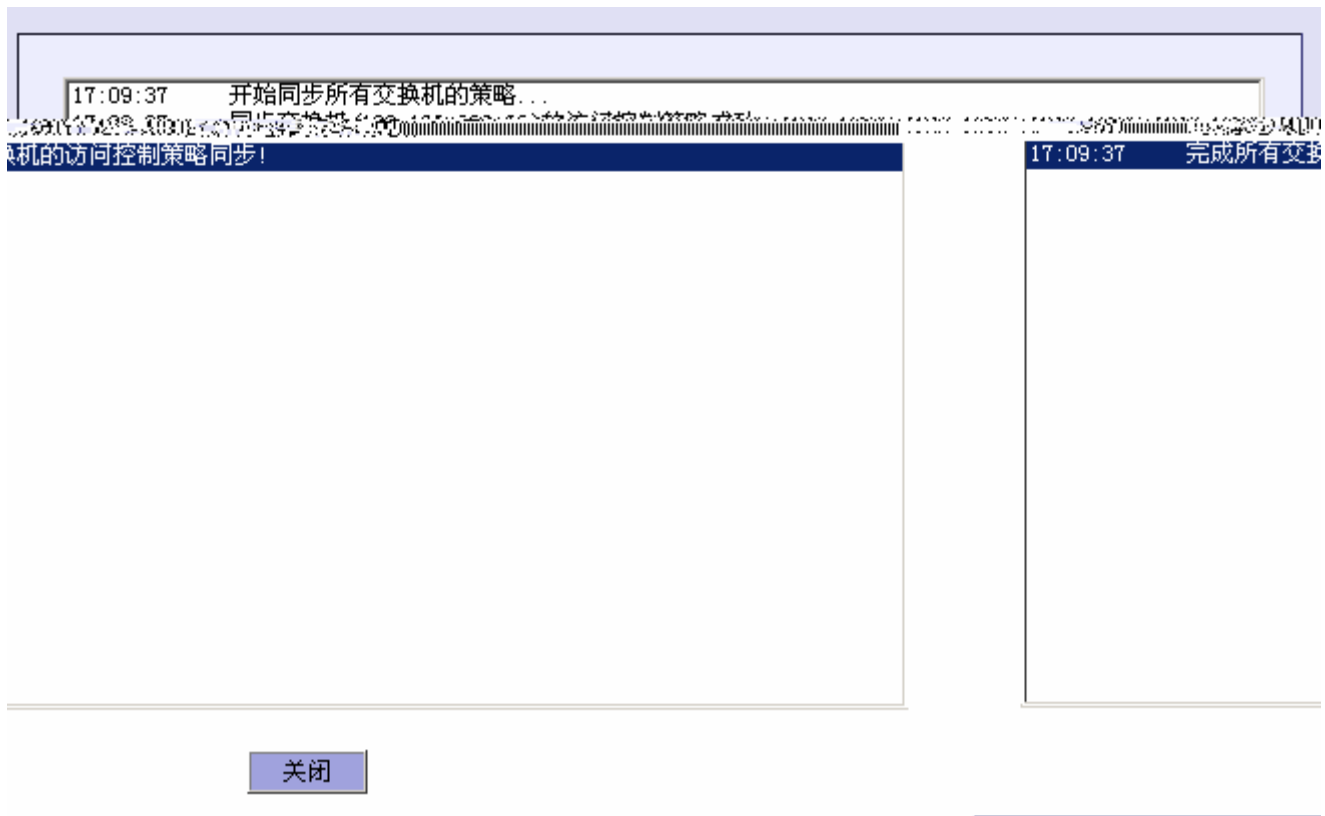
* 访问控制模板组名称:

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
<input type="checkbox"/>	隔离到203网段	隔离		查看
<input checked="" type="checkbox"/>	禁止访问TELNET服务	阻断	禁止用户访问TELNET服务	查看
<input checked="" type="checkbox"/>	禁止访问FTP服务	阻断	禁止用户访问FTP服务	查看
<input checked="" type="checkbox"/>	禁止访问HTTP服务	阻断	禁止用户访问HTTP服务	查看

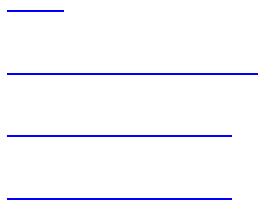
&



说明

2.6

SMP



2.6.1

±

±

MAC

±

±

±

2.6.2

2.6.2.1

%

“

”

“

”

“

”

The screenshot shows a web application interface with search filters and a table of records. The filters include '主机MAC地址' (Host MAC Address) and '应用程序名称' (Application Name). The table has columns for '主机MAC地址', '操作系统平台', '操作系统补丁', and '信息更新时间'. A single record is displayed with MAC address 000C2929928E, Windows XP, Service Pack 2, and an update time of 2009-07-14 00:00:00. Navigation buttons like '删除所选' and '删除全部查询结果' are visible.

主机MAC地址: 应用程序名称:

操作系统平台:

共1条记录 每页20条 第1页/共1页 GO [首页] [上-]

<input type="checkbox"/>	主机MAC地址 ↑	操作系统平台 ↑	操作系统补丁 ↑	信息更新时间 ↑
<input type="checkbox"/>	000C2929928E	Windows XP	Service Pack 2	2009-07-14 00:00:00

详细信息
关联在线用户 查看

&

“

”

“

”

“

”

’

(

∅

”

∅

”

∅

∅



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
最近更新时间:	2009-07-23 17:57:03

更新备注

重置

关闭

应用程序完整列表 ?		应用程序部分列表(共10个)	
应用程序发行商	详情	应用程序名称	应用程序版本
5.51.03	Broadcom	Broadcom 440x 10/100 Integra	
the Ethernet developer commu ity, http://www.ethereal.co	相关搜索	Ethereal 0.10.12	0.10.12
m	相关搜索	Intel (R) Extreme Graphics Dr iver	
Sun Microsystems, Inc.	相关搜索	J2SE Runtime Environment 5.0 Update 5	1.5.0.50
em AMR	相关搜索		
Ruijie Supplicant v3.90	相关搜索	IDM Computer Solutions, Inc.	相关搜索
UltraEdit-32 v14.00a	相关搜索	Politecnico di Torino	相关搜索
WinPcap 3.1 beta4	相关搜索		相关搜索
WinRAR 压缩文件管理器	相关搜索		相关搜索
一键GHOST 8.2 Build 050706	相关搜索		相关搜索



”

(. “ ”

). “ ” “ ”



! . “ ” “ ”

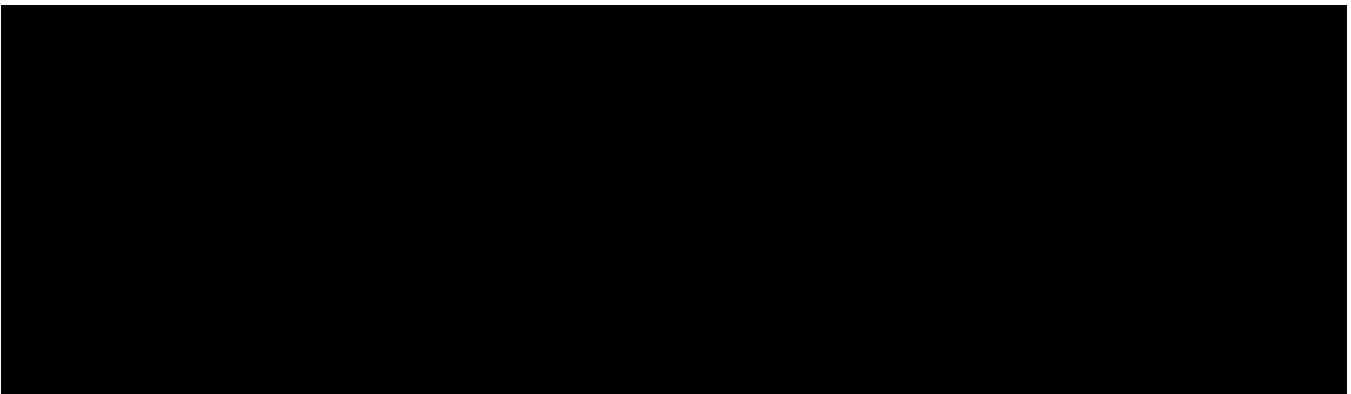
(. “ ”

). “ ” “ ”

2.6.4

2.6.4.1

% “ ” “ ” “ ”



& “ ” “ ” “ ”

! . “ ” “ ”

(.

Ø “ ” “ ”


Ø

Ø “ ” “ ” “ ” “ ”

Ø “ ” “ ” “ ” “ ”

Ø “ ” “ ” “ ”

Ø “ ” “ ” “ ” “ ”

 说明

2.6.4.2

%

“ ” “ ” “ ”

* 应用程序分类名称:

应用程序分类描述:

&

“ ” “ ”

'

“ ”

(

“ ” “ ”

 说明

“*”

2.6.4.3

%

“ ” “ ” “ ”

* 应用程序分类名称:

应用程序分类描述:

&

“ ” “ ” “ ”

'

“ ” “ ”



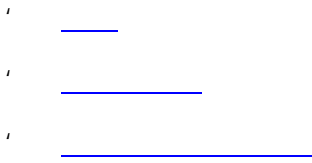
(“ ” “ ”

2.6.4.5

“ ” “ ”

2.7

SMP



2.7.1

SNMP

± SMP SMP
± SMP ARP
±

± [comm word]34A5116E1DA403FE1FF50/Cw54B926

* 交换机IP:

* 是否VRRP部署模式:

↑ 交换机配置标识:

交换机位置:

* 交换机MAC:

交换机名称:

交换机类型:

获取交换机信息 添加 重置 返回

& " " 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	<input type="checkbox"/>	192.168.203.162	wzx16
44	S3750-24	public	查看	<input type="checkbox"/>	192.168.203.198	3750-2
)	S3250-48	public	查看	<input type="checkbox"/>	192.168.203.150	S3250
	S2652G	public	查看	<input type="checkbox"/>	192.168.203.156	xxsf
st	S2628G	public	查看	<input type="checkbox"/>	192.168.203.149	zqd-te
_3	S3760-12SFP	public	查看	<input type="checkbox"/>	192.168.203.214	S3760
h	S2126G	public	查看	<input type="checkbox"/>	192.168.203.178	Switc
e	S2628G	public	查看	<input type="checkbox"/>	192.168.203.174	Ruiji
e	S8606	public	查看	<input type="checkbox"/>	192.168.203.199	Ruiji
760	S5760-24GT/4SFP	public	查看	<input type="checkbox"/>	192.168.203.3	4F_HJ_5
	4F_HJ_5750S	S5750S-24GT/12SFP	public	查看	<input type="checkbox"/>	192.168.203.2
	my switch	S2652G	public	查看	<input type="checkbox"/>	192.168.203.169
	S5760-24GT/4SFP	public	查看	<input checked="" type="checkbox"/>	192.168.203.1	4F_HJ_760
	S2126G	public	查看	<input type="checkbox"/>	192.168.203.90	GSN

“ ” “ ”

%\$ “ ” “ ”

%% “ ” “ ”

%& “ ”

% . “ ”

说明

“**”

2.7.2.4

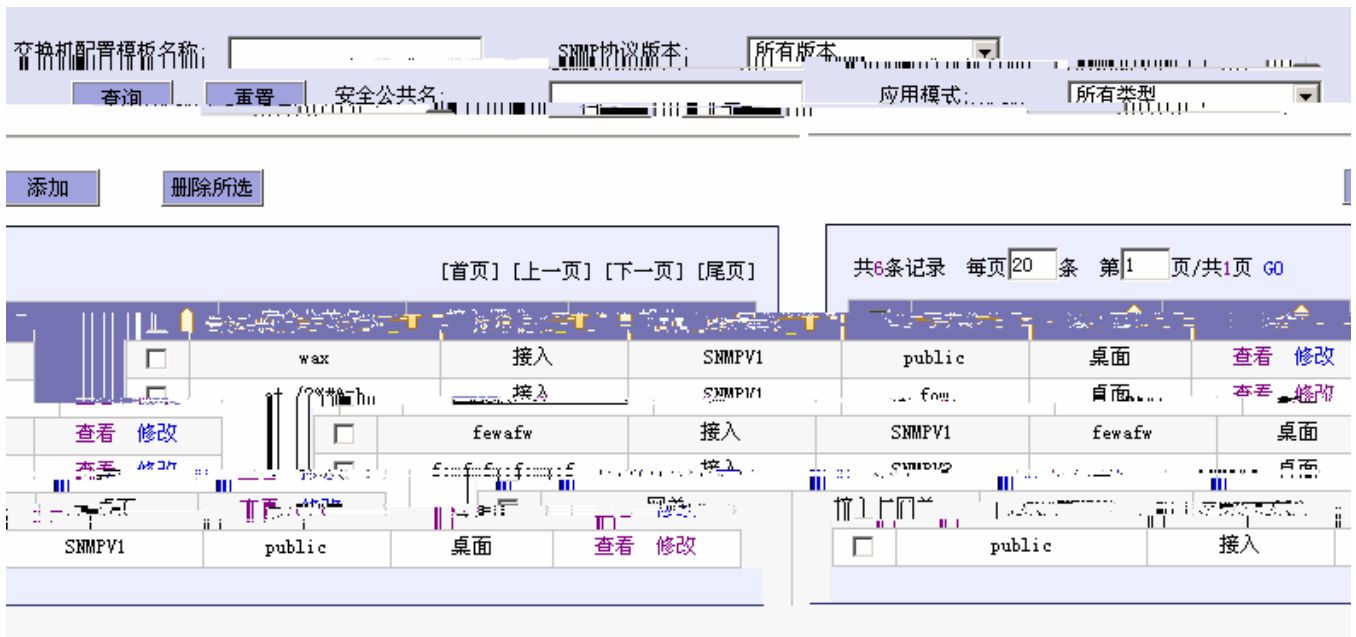
% “ ” “ ” “ ” “ ”

2.7.3

2.7.3.1

%

”



&

“

”

“

”

“

”

,

“

”

“

”

“

(

∅

“

”

“

”

∅

“

”

“

”

“

”

∅

∅

“

”

“

”

“

”

2.7.3.2

%

“

”

“

”

“

”

* 交换机配置模板名称:

* 应用模式:

* 接入模式:

* SNMP协议版本: ?

* 安全公共名: ?

安全策略模板:

用户访问权限:

说明: 如果这里指定了安全策略模板, 那么交换机的用户将应用这里配置的安全策略模板。而如果这里指定了安全策略模板, 那么交换机的用户将应用这里配置的安全策略模板。如果这里指定了安全策略模板, 那么交换机的用户将应用这里配置的安全策略模板。而如果这里指定了安全策略模板, 那么交换机的用户将应用这里配置的安全策略模板。

& “ ” “ ”

“ ”

“ ”

(“ ” “ ”

说明

“*” 64 32

2.7.3.3

% “ ” “ ” “ ”

* 交换机配置模板名称:

* 应用模式:

* 接入模式:

* SNMP协议版本:

* 安全策略模板:

安全策略模板:

用户访问权限:

将应用这里配置的安全策略模板和用户访问权限的模板和用户访问权限的模板和用户访问权限的模板...

1: 如果这里绑定了安全策略模板, 相关交换机上的用户策略模板将失效。
 2: 如果这里绑定了用户访问权限, 相关交换机上的用户访问权限将失效。
 3: 如果交换机配置模板正在被在线用户使用, 安全策略修改将在用户下次访问时生效。

& " " " "

" "

' " "

(" " " "

说明

/**

2.7.3.4

" " " "

说明

- '
- '
- '
- '
- '

2.8.1

±

±

±

±

SMP

SQL Server

说明

2.8.2

-

8

-

2

“

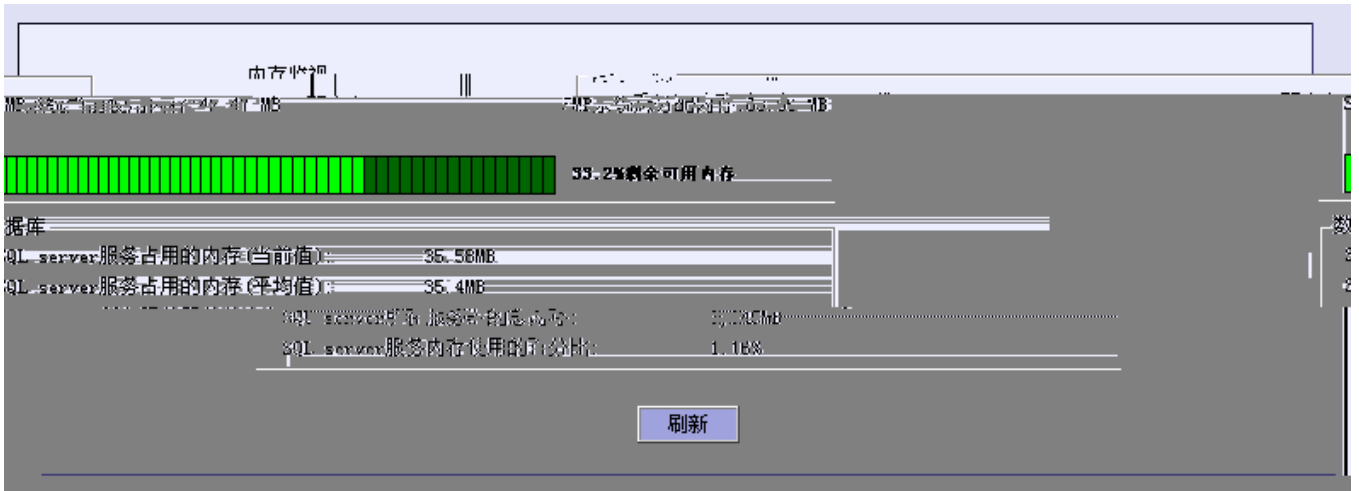
”

“

”

“

”



& “ ”

2.8.4

% “ ” “

2.8.5

%

“ ” “ ” “ ”

自动删除一周前记录

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]

交换机IP ↑	发送报文数 ↑	最后发送报文时间 ↑	操作
192.168.203.37	1	2009-07-07 16:43:56	Telnet 添加交换机 删除

&

“ ”

'

“Telnet” telnet

(

“ ” “ ” “ ” “ ” “ ” “ ” “ ”

)

“ ”

2.9

SMP

—
—

2.9.1

±

SMP

SMP

±

SAM

IP

SMP

±

SMP

±

±

±

IP SMP
IP

“ ”

127.0.0.1 192.168.1.2

127.0.0.1

±

/ /

SMP

SMP

9090

±

5

±

120

±

SMP

SMP

SMP

60

±

2.9.2

%

“ ”

“ ”

SMP

接入用户控制

定期检测用户在线状态

* SAM服务器IP:

注意: 可以配置多个SAM服务器(IP地址不能使用MLB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: 分钟(默认为60分钟)

* 配置文件更新服务器:

配置文件更新服务器是指存放锐捷安全认证客户端初始化配置的FTP服务器地址, 地址的根目录指向SMP安装目录下的dat文件夹。

网络攻击防治

开启网络攻击防治

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 <= % 时直接丢弃

* 可信度 <= % 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 <= % 时直接丢弃

* 可信度 <= % 时只记录日志

* 安全事件解析服务器:

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, 192.168.2.23”。

其他功能

- * 第三方系
- * 端点防护
- * 软硬件配
- * 访问控制
- * 修复服务

访问端口: (默认为9090)

状态检测周期: 分钟(默认为5分钟)

置信息报告周期: 分钟(默认为120分钟)

策略同步周期: 分钟(默认为60分钟)

器:

2.10

SMP

2.10.1

SMP

± “ ”

± “ ”

± “ ”

± “ ” SMP

± “ ”

± “ ”

±

±

± SMP “system”

±

 说明

2.10.2

2.10.2.1

%

“ ” “ ”

日志类型:




日志的创建时间(开始):

日志内容:

日志的创建时间(结束):

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

<input checked="" type="checkbox"/>	自动删除 (1~360)*	180	天以前的端点防护日志
<input checked="" type="checkbox"/>	自动删除 (1~360)*	180	天以前的安全日志
<input checked="" type="checkbox"/>	自动删除 (1~360)*	180	天以前的操作日志
<input checked="" type="checkbox"/>	自动删除 (1~360)*	180	天以前的系统日志
<input checked="" type="checkbox"/>	自动删除 (1~360)*	180	天以前的客户端信息日志
<input checked="" type="checkbox"/>	自动删除 (1~360)*	180	天以前的敏感资源防护日志

& “ ” “ ” “ ”

’ “ ”

(“ ” “ ”

说明

’

2.11.1

±
±
±
±
±
±
±
±
±
±

TOP N
TOP N
TOP
TOP

2.11.2

2.11.2.1

%
&
'



(
)
*

说明

12

2.11.2.2

%

&

'

(

)

*

说明

,

,

2.11.2.3

%

&

'

* 开始月份: 年 月

* 结束月份: 年 月

安全事件类型TOP: (默认值为10)

交换机TOP: (默认值为10)

开始日期:

* 结束日期:

安全事件类型TOP: (默认值为10)

交换机TOP: (默认值为10)

(. “ ” “ ”)

).

*. “ ” “ ”

 说明

2.11.2.4

%

& “ ” “ ”

! “ ” “ ” “ ”

15

15

* 结束日期:

* 安全事件类型TOP: (默认值为10)

* 交换机TOP: (默认值为10)

(. “ ” “ ”)

).

*. “ ” “ ”

* “ ” “ ”

说明

2.11.2.5 ()

%

& “ ” “ ”

“ ” “ ” ()” “ ()”

* 开始日期:

* 结束日期:

安全事件类型TOP: (默认值为10)

(“ ” ()” ()
“ ” N

) “ ”

* “ ” “ ”

说明

2.11.2.6 ()

%

&

“ ” “ ”

“ ” “ ” () “ ” ()

* 开始日期:

* 结束日期:

交换机TOP: (默认值为10)

(“ ” ()) () “ ” i

说明

2.11.2.8

% “ ” “ ” “ ”

此功能用于生成硬件分布情况报表

生成报表

返回

& “ ” “ ”

' “ ” “ ”

3 FAQ

1.

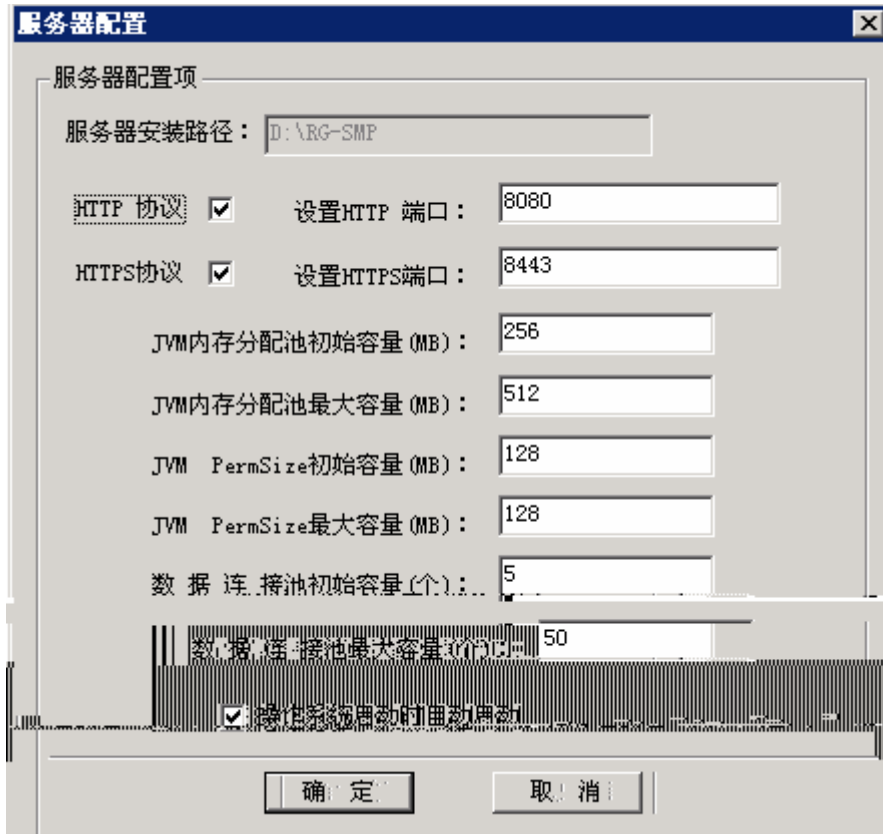
SMP <http://127.0.0.1:8080/smp/index.jsp>
admin 1111111111

2.

SMP
IP

3.

SMP HTTP HTTPS
“ / ”
HTTP HTTPS



4. “ ” session
 SMP IE “ ” “ ”
 IE SMP

5. “ ” session
 SMP

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