

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

- o SAM
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o 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

☒ 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 <= 80 % 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 <= 80 % 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, 192.168.2.23”。

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

“ ” “ ” “ ”

基本信息

权限控制方式

板名称	描述	操作
系统		查看
网络资源		查看

添加

重置

返回

控制方式

☐ 不控制 ☒ 上网控制

控制策略

☒	上网权限模
☒	允许访问日
☒	禁止访问所有

“ ”

1.2.3

“ ”

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	江民2008及以后的版本	强联动	杀毒引擎 病毒库
不检查			☐ 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	☐ 查看 修改	江民杀毒软件KV2007	弱联动	杀毒引擎 病毒库
不检查			☐ 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	☐ 查看 修改	卡巴斯基互联网安全套装6.0个人版	弱联动	杀毒引擎 病毒库
不检查			☐ 查看 修改	卡巴斯基互联网安全套装6.0个人版	弱联动	杀毒引擎 病毒库
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 病毒库
不检查			☐ 查看 修改	卡巴斯基反病毒7.0个人版	弱联动	杀毒引擎 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 病毒库
不检查			☐ 查看 修改	Symantec AntiVirus企业版 8	弱联动	杀毒引擎 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 病毒库
不检查			☐ 查看 修改	Symantec AntiVirus企业版 9	弱联动	杀毒引擎 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 病毒库
不检查			☐ 查看 修改	Symantec AntiVirus企业版 10	弱联动	杀毒引擎 病毒库
检查	自适应顺延天数	7	☐ 查看 修改	安博士杀毒软件 V3 VirusBlock2005	弱联动	杀毒引擎 病毒库
不检查			☐ 查看 修改	安博士杀毒软件 V3 VirusBlock2005	弱联动	杀毒引擎 病毒库
检查	自适应顺延天数	7	☐ 查看 修改	McAfee VirusScan V10.0	弱联动	杀毒引擎 病毒库
不检查			☐ 查看 修改	McAfee VirusScan V10.0	弱联动	杀毒引擎 病毒库
检查	自适应顺延天数	7	☐ 查看 修改	McAfee VirusScan Enterprise 8.5.0i	弱联动	杀毒引擎 病毒库
不检查			☐ 查看 修改	McAfee VirusScan Enterprise 8.5.0i	弱联动	杀毒引擎 病毒库
检查	自适应顺延天数	7	☐ 查看 修改	NOD32 2.5	弱联动	杀毒引擎 病毒库
不检查			☐ 查看 修改	NOD32 2.5	弱联动	杀毒引擎 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 病毒库
不检查			☐ 查看 修改	NOD32 2.7	弱联动	杀毒引擎 病毒库

基本信息

杀毒软件名称:

自适应

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

扫描

☒ 上报不能清除的病毒信息

* 全盘扫描时间间隔: 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

信息:

验证地址

修改

重置

返回

☐ 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

病毒扫描

☒ 认证后立即执行内存扫描

☒ 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://[]:[]@[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, 192.168.1.24”

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

☒ 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访问

* 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访问

* 可信度 <=

% 时直接丢弃

* 可信度 <=

% 时只记录日志

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5分钟)

* 访问控制策略同步周期:

5

分钟 (默认为60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ftp://, https://或http://开头

修改

重置

1.4

PC

RG-SMP

1.1

“ ” “ ”



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

“

1

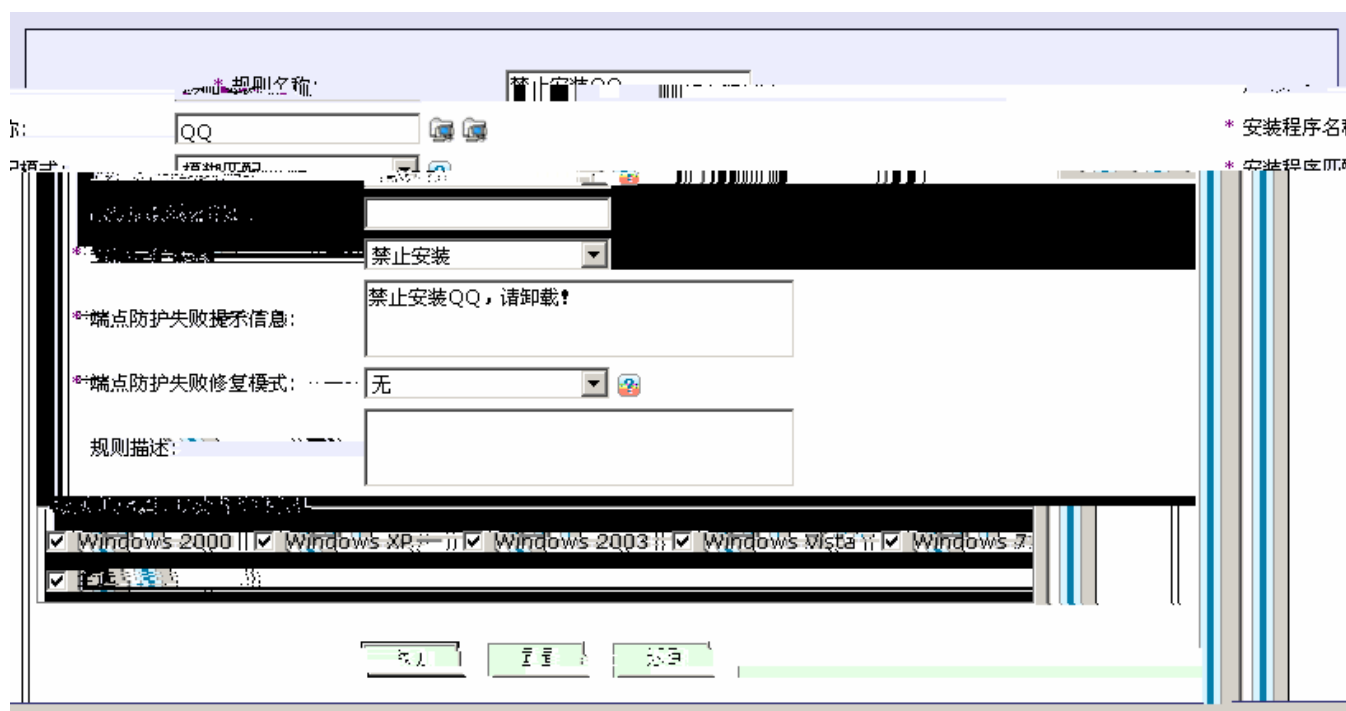
"

“

,

“

"



“

"

* 规则名称: 禁止启动BQQ

* 进程名称: RTX

* 运行状态: 禁止运行

* 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 ☒ Windows Vista ☒ Windows 7

☒ 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防火墙，为了更好的访问网络，请开启windows防火墙！

* 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 ☐ Windows 7

☐ 全选

修改 重置 返回

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

☒	规则名称	规则类型	相应对象名称	相应对象状态	详细信息
☒	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	查看

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

RG-SMP PCMCIA

U

PC

1.6.1

[1.1](#)

1.6.2

“ ”

设备信息

配置向导

外联接口控制

软硬件配置信息收集

安全策略处理

外联接口名称	控制方式	提示信息
PCMCIA接口	强制禁用	禁止使用PCMCIA接口！
串口	强制禁用	禁止使用串口！
智能卡读卡器	强制禁用	禁止使用智能卡读卡器！
红外线接口	强制禁用	禁止使用红外线接口！
打印机	强制禁用	禁止使用打印机！
磁带机	强制禁用	禁止使用磁带机！
软盘驱动器	强制禁用	禁止使用软盘驱动器！
光盘驱动器	强制禁用	禁止使用光盘驱动器！

禁止使用U盘！

U盘=强制禁用

回

添加

重置

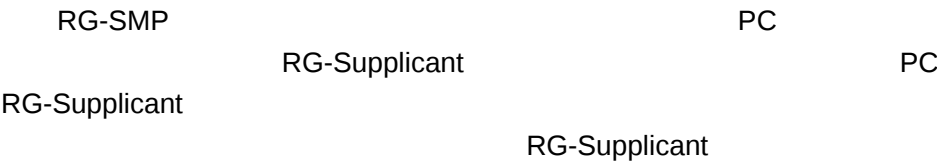
退

注意：重置功能将重置所有选项卡中的信息。

1.6.3

[1.3.5](#)

1.7



1.7.1

[1.1](#)

92

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:

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, 192.168.1.24”。配置成功后, 你可通过“系统日志”->“通讯端口”->“安全事件”->“SAM服务器的启动与关闭”来查看。

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

配置文件更新服务器是指存放给安全认证客户端初始化的配置的FTP服务器地址。地址的根目录指向SAM安装目录下的conf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 <= 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, 192.168.1.24”。

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)

* 访问控制策略同步周期:

5

分钟 (默认为120分钟)

* 修复服务器:

http://192.168.6.194

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。

重置

修改

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	☒	☒	查看	192.168.203.1	00D0F8BC9511		
接入与网关	☒	☐	查看	192.168.203.150	00D0F82233AD	S3250	S3250-48
接入与网关	☒	☐	查看	192.168.203.156	00D0F8223389	xsf	S2652G
接入与网关	☒	☐	查看	192.168.203.161	001AA918E617	Ruijie	S2628G
接入与网关	☒	☐	查看	192.168.203.163	00D0F8EDCD5A	xsf	其它类型
S2652G	接入与网关	☒	☐	查看	192.168.203.169	00D0F82233AF	my switch
S3750-24	接入与网关	☒	☐	查看	192.168.203.172	00D0F8C7A4E1	Ruijie
S8606	接入与网关	☒	☐	查看	192.168.203.199	00D0F812341B	Ruijie
S2150G	接入与网关	☒	☐	查看	192.168.203.254	00D0F8BF9EB4	apache
S2126G	接入与网关	☒	☐	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	☒	☒	查看
192.168.203.150	00D0F82233AD	S3250	S3250-48	接入与网关	☒	☐	查看
192.168.203.156	00D0F8223389	xsf	S2652G	接入与网关	☒	☐	查看
192.168.203.161	001AA918E617	Ruijie	S2628G	接入与网关	☒	☐	查看
192.168.203.163	00D0F8EDCD5A	xsf	其它类型	接入与网关	☒	☐	查看
192.168.203.169	00D0F82233AF	my switch	S2652G	接入与网关	☒	☐	查看
192.168.203.172	00D0F8C7A4E1	Ruijie	S3750-24	接入与网关	☒	☐	查看
192.168.203.199	00D0F812341B	Ruijie	S8606	接入与网关	☒	☐	查看
192.168.203.254	00D0F8BF9EB4	apache	S2150G	接入与网关	☒	☐	查看
GSN	S2126G	接入与网关	☒	☐	查看	192.168.203.90	00D0F8BC9556

- 说明
- o “ ARP ”

ARP

o “ ARP ”

ARP

ARP

2

Red-Giant Security Management Platform SMP)

SMP

- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____
- o _____

2.1

SMP

- o _____
- o _____
- o _____
- o _____
- o _____

2.1.1

SMP

×	-----	SMP	supervisor
	ruijiesmp		
×	-----	SMP	log
	111111111		
×	-----	SMP	
	SMP	admin	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:

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

“ ” “ ” “ ”

“ ” “ ”

p “ ” “ ” “ ”

p “ ” “ ”

p

p “ ” “ ” “ ”

 说明

2.1.5.2

“ ” “ ” “ ” “ ”



- o _____
- o _____
- o _____
- o _____

2.2.1

- x _____, RG-SAM
_____, _____
- x _____
- x _____
- x _____
1 2 1
- x _____
1 2 1

2.2.2

SMP SAM SMP

2.2.2.1

“ ” “ ” “ ”

2.2.2.3

强制下线消息配置

强制下线消息

你已被强制下线!

强制下线

重置

关闭

 说明

0

2.2.2.4

 说明

0

说明

o

o

2.2.2.6

“ ” “ ” “ ”

消息内容:

修复程序类型:

下载补丁

?

无

?

* 修复程序URL:

验证URL

下发

重置

关闭

“ ”

“

“

“

o

URL

URL

“ ”

2.2.3

SMP

2.2.3.1

“ ” “ ” “ ” “ ”

用户组名称:

安全策略模板:

用户组描述:

用户访问权限:

查询

重置

用户组名称

用户组描述

操作

默认用户访问权限

修改

默认用户访问权限

修改

默认用户访问权限

修改

默认用户访问权限

系统默认的用户组1

修改

共4条记录 每页20条 第1页/共1页 GO

用户组名称

安全策略模板

领导组

default

老师组

default

学生组

default

默认用户组

default

“ ” “ ” “ ” “ ”

“ ” “ ”

p “ ” “ ” “ ”

p “ ” “ ”

p

p

p “ ” “ ” “ ” “ ”

”

39 133 39

 说明

o

2.2.3.2

“ ” “ ” “ ”

* 用户组名称:

* 安全策略模板:

未选择

* 用户访问权限:

未选择

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。

添加

重置

返回

“ ”

“ ”

“ ”

“ ”

“ ”

“ ”

“ ”

 说明

o “*”

32

16

o

2.2.3.3

“ ”

“ ”

“ ”

* 用户组名称:	领导组
* 安全策略模板:	default
* 用户访问权限:	默认用户访问权限
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。

修改

重置

返回

 说明

2.2.3.4

 说明

2.2.4

2.2.4.1

用户访问权限名称:

控制方式:

所有控制方式

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]

☐	用户访问权限名称 ↑	控制方式 ↑	操作
☐	默认用户访问权限	不控制	查看 修改

p

p

p

p

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

- O

“*”

32

16
- O
- O

“ ”
- O

“ ”
- O

“ ”

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

网络资源名称

☒ 允许访问日志系统

☒ 禁止访问所有网络资源

如果用户访问权限正在被在线用户使用, 您的修改将在用户下次认证时生效

修改

重置

返回

“

”

“

”

“

”

“

”

“

”

“

”

“

”



说明

o

o

2.2.4.4

“

”

“

”



说明

o

o

2.2.5

SMP

2.2.5.1

安全策略模板名称：

安全策略模板描述：

查询

重置

高级查询

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]

	安全策略模板名称 	安全策略模板描述	操作
	安全策略模板名称	安全策略模板描述	   

p “ ” “ ” “

_____ ”

p “ ” “ _____

”

p

p “ ” “ ”

_____ ”

2.2.5.2

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

* 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。

“ ”

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

☐ 启用端点防护

端点防护策略模板: 未选择

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:

非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！

添加

重置

返回

注意：重置功能将重置所有选项卡中的信息。

46

133

46

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。



安全审计处理		安全审计处理	
		应用安全措施	

“	”	“	”	“	”
“	”				
“	”	“	”		



说明

O	“*”	32	16
O			
O			
O			“ ”
O			
O	“ ”		“
			”
O			
O			

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

o

o



“ ” “ ”
o

2.2.5.4

“ ” “ ”
 说明
o

2.3

	SMP
o	
o	
o	
o	
o	

2.3.1

×
“ 2008 ”
×

×

×

X

x

2.3.2

SMP

2.3.2.1

端点防护策略模板名称：

用户组：

模板名称

是否启用微软补丁更新

操作

添加

删除所选

操作	端点防护策略模板名称	描述	是否启用微软补丁更新
查看 修改	禁止运行cmd.exe		否

p

p

p

p

说明

0

2.3.2.2

“”“”“”“”“”“”

端点防护策略模板名称

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

端点防护策略模板描述

返回

添加

重置

删除

注意：重置功能将重置所有选项卡中的信息。

O	“*”	32	16
O			
O			

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

策略模板描述:

策略模板具体信息请查看各标签卡项

端点防护策略模板重置功能

端点防护策略模板重置功能

端点防护策略模板重置功能

端点防护策略模板重置功能

端点防护策略模板重置功能

端点防护策略模板重置功能

端点防护策略模板重置功能

端点防护策略模板重置功能

“”

“”

“”

“”

“”

“”

“”

“”

“”

“”

 说明



--	--



2.3.3.1

“ ” “ ” “ ”



p

“ ”

“

”

“

”

2.3.3.2

“

”

“

”

“

”

规则组名称:

规则组类型:

所有类型

端点防护策略模板名称:

规则名称:

查询

重置

添加

删除所选

返回

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]

	规则组名称 ↑	规则组描述	规则组类型 ↑	操作
	禁止运行cmd.exe		必备	查看 修改 修改绑定

“ ” “ ” “ ”

“ ” “ ”

p “ ” “ ” “ ”

p “ ” “ ”

p

p “ ” “ ” “ ”

p “ ” “ ” “ ”



说明

o

2.3.4.2

“ ” “ ” “ ”

“ ”

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
* 规则组类型:	可选
▼ ?	
* 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

O

2.3.4.4

 说明

o

2.3.4.5

“ ” “ ” “ ”

规则组：可以使用QQ

	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

“ ”

“ ” “ ” “ ”

“ ”

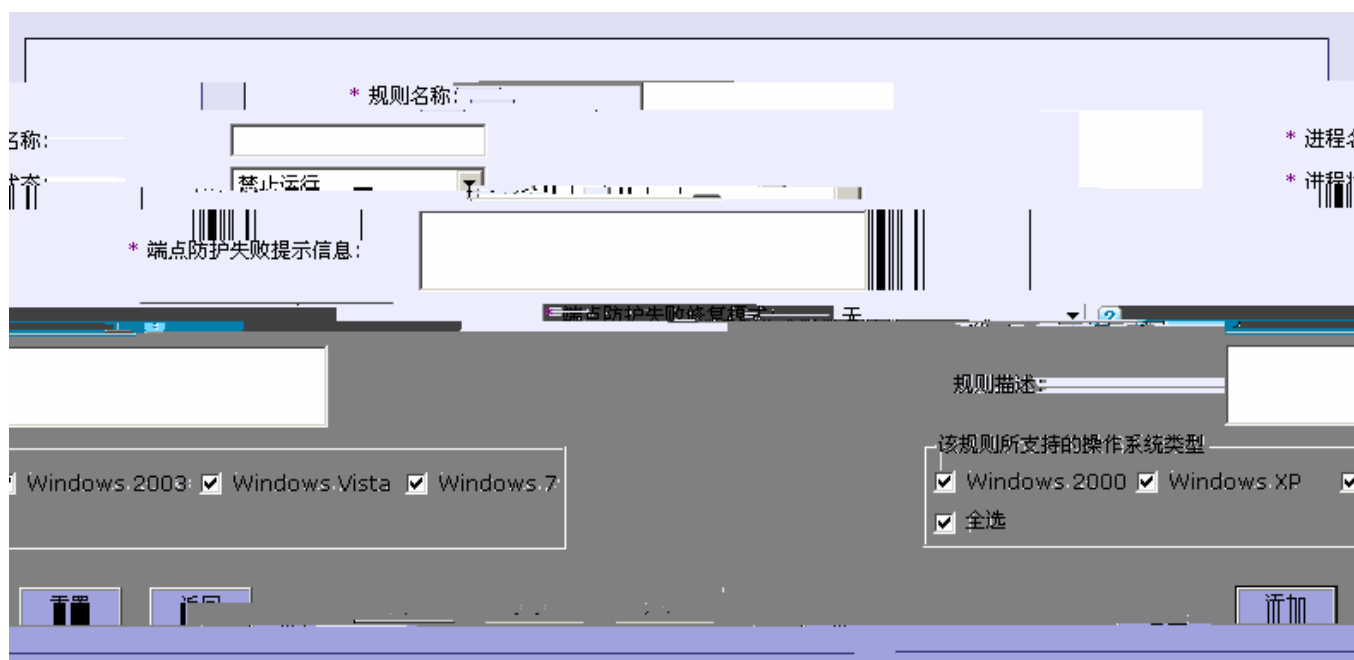
“ ” “ ”

2.3.5

SMP

2.3.5.1

“ ” “ ” “ ” “ ” “ ”



 说明

- | | | | |
|---|-------|-----|----|
| 0 | "{x}" | 128 | 64 |
| 0 | | | |
| 0 | | | |

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:

REG_DWORD

键值表达式:

小于

注册表键值:

* 注册表状态:

禁止存在

* 端点防护失败提示信息:

* 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

添加

重置

返回

“

”

“

”

“

”

“

”

“

”

“

”



说明

O

“*”

128

64

O

O

“

”

O

“

”

O

“

”

* 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 Vista

☒ 全选

添加

重置

返回

 说明

64

O

2.3.5.6

“	”	“	”	“	”
“	”				
“	”	“	”	“	”
“	”				
“	”	“	”		

 说明

0

2.3.5.7

“	”	“	”
---	---	---	---

 说明

0

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

“	...”
---	------



说明

0

10M

0

SMP

0

2.3.5.9

规则组名称

规则组类型

所有类型

导出

返回

☐	规则组名称	规则组描述	规则组类型	操作
☐	禁止运行cmd.exe		必备	查看
☐	可以使用qq		可选	查看

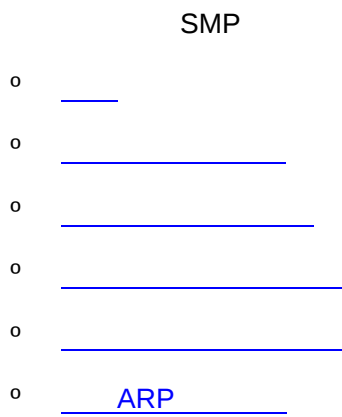


说明



o	
o	.dat

2.4



2.4.1



2.4.2



2.4.2.1

“ ” “ ” “ ”

The diagram illustrates a sequence of 12 steps arranged in a 3x4 grid. The steps are numbered 1 through 12. Steps 1, 3, 5, 7, 9, and 11 are marked with a blue horizontal line. Steps 2, 4, 6, 8, 10, and 12 are marked with a blue vertical line.

O

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
查看 修改	☐ HTTP_CGI_Phorum_HTTP应答分割攻击	重要	0	应用攻击频率处理模式
查看 修改	☐ HTTP_alibaba.pl_任意命令执行尝试	普通	0	应用攻击频率处理模式
查看 修改	☐ SUNRPC_ToolTalk溢出尝试	严重	0	应用攻击频率处理模式
查看 修改	☐ HTTP_bb-histlog.sh_访问	普通	0	应用攻击频率处理模式
查看 修改	☐ SMTP_RCPT_TO_decode_尝试	普通	0	应用攻击频率处理模式
查看 修改	☐ SMTP_W32.Sober.I_蠕虫病毒	重要	0	应用攻击频率处理模式
查看 修改	☐ SUNRPC_ttdbserv溢出尝试	严重	0	应用攻击频率处理模式
查看 修改	☐ TM&P.Inswitch.IMail.Del...	严重	0	应用攻击频率处理模式
查看 修改	☐ 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_rwallld进程请求	通知	0	应用攻击频率处理模式
查看 修改	☐ SUNRPC_vnserv.manlist_请求(TCCL	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

p

```

p      "      "
      "      "
p      "      "
      "      "
p      "      "      "      "
p
p
p      "      "      "      "      "
      "

```

说明

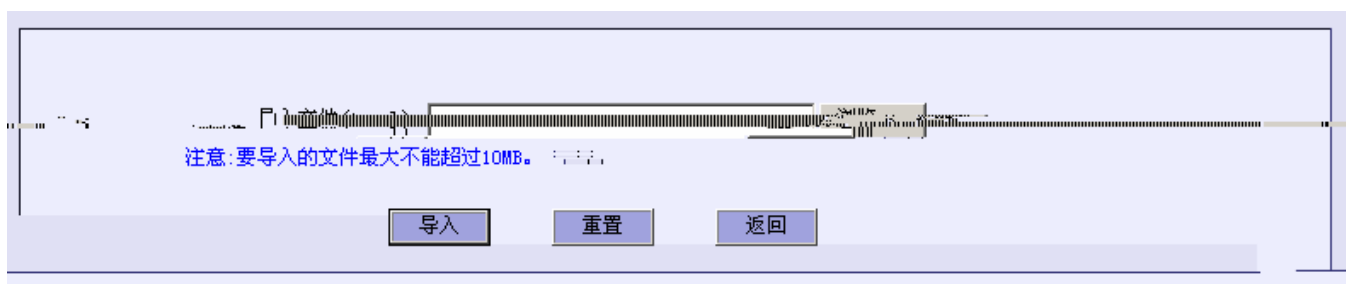
o

2.4.3.2

```

"      "      "      "      "      "

```



```

"      "
...
"      "
"      "
"      "      "      "

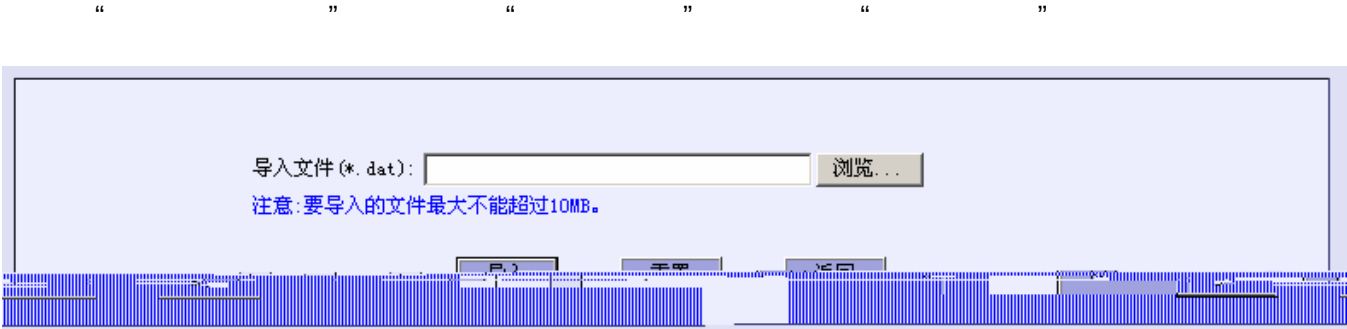
```

说明

o 10M

o 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。
“熊猫烧香”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

“ ”

“ ” “ ”

80

133

80

返回

O

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”病毒最早全能在Win 9X/2000/XP/2003系统上运行的蠕虫病毒。病毒体只有30-40K左右,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

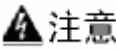
安全事件类型描述:
解决方案:
+请把杀毒软件
参考文献:
+N/A

更至最新版本并查杀病毒

修改

告警

返回



0



2.4.3.7

“ ” “ ”

 说明

O “ ”

2.4.5.1

安全事件处理模板名称:

模板描述:

查询

重置

添加

删除所选

安全事件处理模板名称 	处理模式	模板描述	操作
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
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

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!)

添加

重置

返回

“ ”

“ ” “ ” “ ”

”

“ ”

“ ” “ ”

 说明

- O “*” 64 32
- O
- O “
- ”
- “ ”

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
☐	隔离到203网段	隔离		查看

修改

重置

返回

 说明

0

2.4.5.4

 说明

o

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
☐	查看	192.168.203.149	001AA90F9163	zqd-test	S2628G	接入与网关	☒

“ ”

“ ARP ” ARP

“ ARP ” ARP

“ ARP ” ARP

 说明

o

ARP

o

“

>

”

ARP

ARP

2.5

SMP

o

o

o

o



o



2.5.1

x

x

x

x

HTTP FTP

策略编号:

用户名:

用户IP:

交换机IP:

目的IP:

查询

重置

高级查询

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]

	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
查看 修改	☐	10396	阻断	192.168.203.90		1.1.1.3		是

“ ” “ ” “ ”

”

“ ” “ ”

p “ ” “ ” “ ”

_____”

p “ ” “ ”

p “ ” “ ”

p “ ” “ ”

p “ ” “ ” “ ”

_____”

说明

o

2.5.2.2

“ ” “ ” “ ” “ ”

2.5.3.2

* 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
添加 重置 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:	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

0 “*”

32

16

0

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

0 “*”

32

16

0

2.5.3.5

* 访问控制模板名称:		
* 访问模式:		未选择
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	
是否使用时间调度:	否	
添加 重置 返回		

 说明



O	“★”	32	16
O			
O	“ ” “ ”		
O	“ ”		

2.5.3.6

“ ”	“ ”	“ ”	“ ”
“ ”	“ ”		
“ ”	“ ”	“ ”	“ ”
“ ”	“ ”		
“ ”	“ ”	“ ”	“ ”

 说明

O			
O			
O	“ ” “ ” “ ”	“ ”	
	“ ”	“ ”	

2.5.3.7

“ ”	“ ”	“ ”	“ ”
 说明			
O			

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]

☐	访问控制模板组名称 ↑	访问控制模板组描述	操作
☐	禁止访问网络		查看 修改

p

p

p

p

 说明

o

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

☐	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
☐	禁止访问HTTP服务	阻断	禁止用户访问Http服务	查看

添加

重置

返回

“ ”

“ ”

“ ”

“ ” “ ” “ ” “ ”

 说明

- O

“*”

32

16
- O
- O

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:

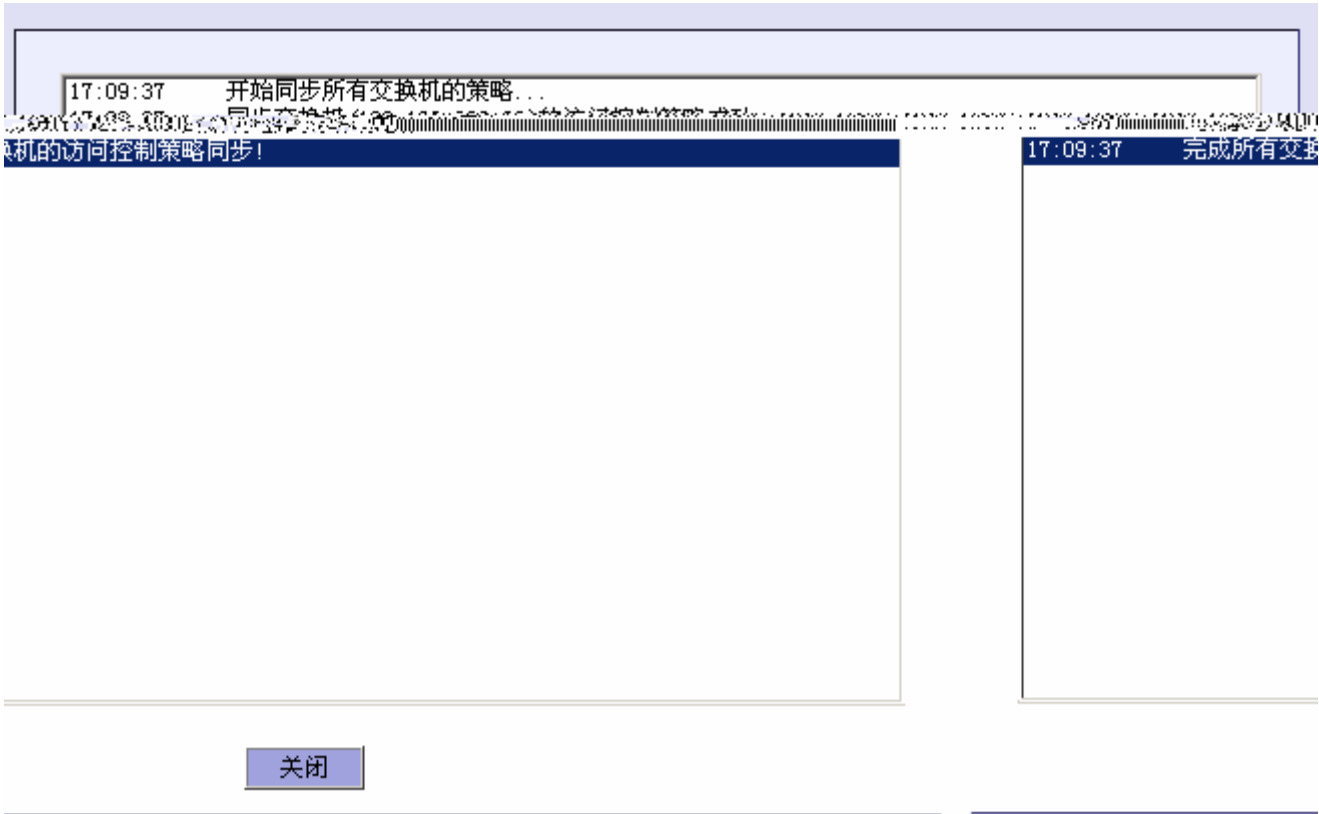
访问控制模板

☐	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
☒	禁止访问SSH服务	阻断	禁止用户访问SSH服务	查看

修改

重置

返回



说明

o

2.6

SMP

- o
- o
- o
- o

2.6.1

x

x

MAC

×

×

×

2.6.2

2.6.2.1

主机MAC地址：

应用程序名称：

删除所选

删除全部查询结果

前一页

下一页

尾页

详细信息

关联在线用户

查看

共1条记录

每页20条

第1页/共1页

GO

首页

上一页

☐	主机MAC地址 ↑	操作系统平台 ↑	操作系统补丁 ↑	信息更新时间 ↑
☐	000C2929928E	Windows XP	Service Pack 2	2009-07-14 00:00:00

p

p

p

p



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:	2009-07-22 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 Ethereum developer commu	相关搜索	Ethereal 0.10.12	0.10.12
ity, http://www.ethereal.co	相关搜索	Intel (R) Extreme Graphics Dr	
m	相关搜索	iver	
Sun Microsystems, Inc.	相关搜索	J2SE Runtime Environment 5.0	1.5.0.50
		Update 5	
em AMR			
Ruijie Supplicant v3.90	相关搜索	IDM Computer Solutions, Inc.	相关搜索
UltraEdit-32 v14.00a		Politecnico di Torino	相关搜索
WinPcap 3.1 beta4			相关搜索
WinRAR 压缩文件管理器			相关搜索
一键GHOST 8.2 Build 050706			相关搜索



11

11 11

11 11 11 11

”

“ ” “ ”

p “ ” “ ”

p “ ” “ ”

p “ ” “ ”

p “ ” “ ”

p “ ” “ ”

p “ ” “ ”

google



o

2.6.3.2

“ ” “ ”

“ ” “ ”

2.6.3.3

“ ” “ ” “ ”

”

应用程序：Hotfix for Microsoft .NET Framework 3.5 SP1 (KB958484)		
选择	应用程序分类名称	应用程序分类描述
取消绑定	重置	返回
绑定		

“ ” “ ” “ ”

“ ”



“ ”

“ ”

“ ”

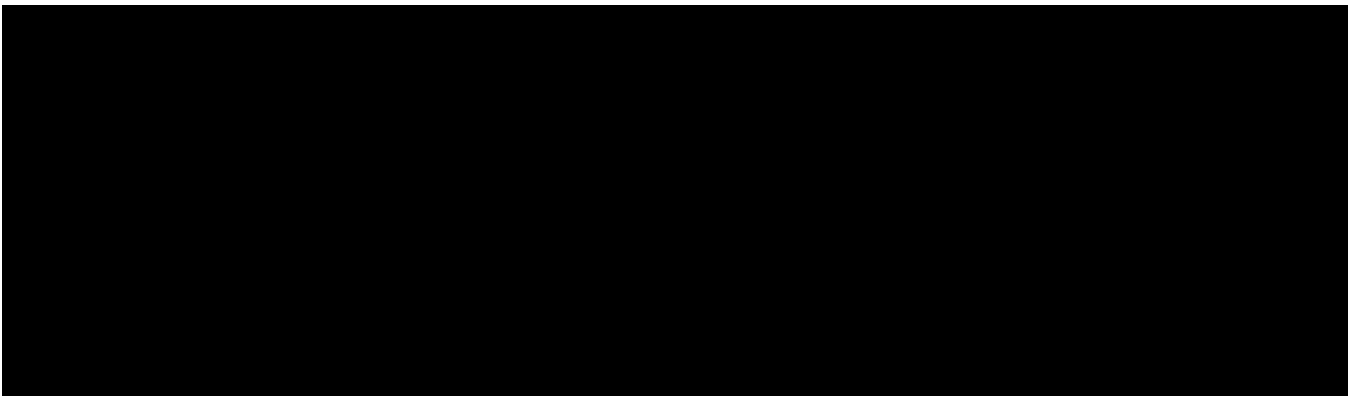
“ ” “ ”

2.6.4

2.6.4.1

“ ” “ ” “ ” “ ” “ ”

”



“ ” “ ” “ ” “ ” “ ”

”

“ ” “ ” “ ” “ ”

p “ ” “ ”

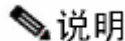
p

p “ ” “ ” “ ” “ ” “ ”

p “ ” “ ” “ ” “ ” “ ” “ ”

p “ ” “ ” “ ” “ ” “ ”

p “ ” “ ” “ ” “ ” “ ”



O

2.6.4.2

* 应用程序分类名称:

应用程序分类描述:

添加

重置

返回



Q “*”

2.6.4.3

应用程序分类名称:

微软更新补丁

应用程序分类描述:

修改

重置

返回



“

”

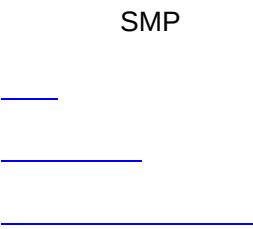
“

”

2.6.4.5

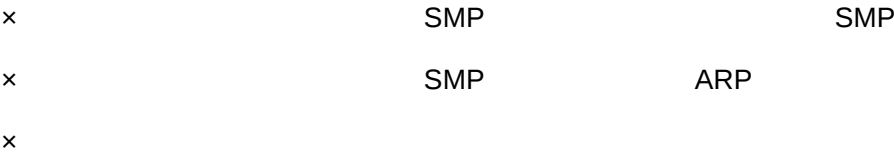
“ ” “ ”

2.7



2.7.1

SNMP



x [comm word]34A5116E1DA403FE1FF50/Cw54B926

交换机IP：

交换机名称：

交换机配置模板：

所有配置模板

交换机类型：

所有类型

查询

重置

高级查询

添加

批量添加

删除所选

同步访问控制策略

同步全部查询结果的MAC

共1条记录 每页20条 第1页/共1页 GO

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

p			
p			
p			
p			
p		MAC	MAC
p			
p			
p			
p			

2.7.2.2

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
44	S3750-24	public	查看
5	S3250-48	public	查看
	S2652G	public	查看
st	S2628G	public	查看
_3	S3760-12SFP	public	查看
h	S2126G	public	查看
e	S2628G	public	查看
e	S8606	public	查看
760	S5760-24GT/4SFP	public	查看

4F_HJ_5750S	S5750S-24GT/12SFP	public	查看
my switch	S2652G	public	查看
S5760-24GT/4SFP	public	查看	
S2126G	public	查看	

☐	192.168.203.162	wzx16
☐	192.168.203.198	3750-2
☐	192.168.203.150	S3250
☐	192.168.203.156	xsxf
☐	192.168.203.149	zqd-te
☐	192.168.203.214	S3760
☐	192.168.203.178	Swite
☐	192.168.203.174	Ruiji
☐	192.168.203.199	Ruiji
☐	192.168.203.3	4F_HJ_5
☐	192.168.203.2	
☐	192.168.203.169	
☒	192.168.203.1	4F_HJ_760*
☐	192.168.203.90	GSN

“ ”

“ ”

“ ”

“ ”

“ ”

“ ”

“ ”

说明

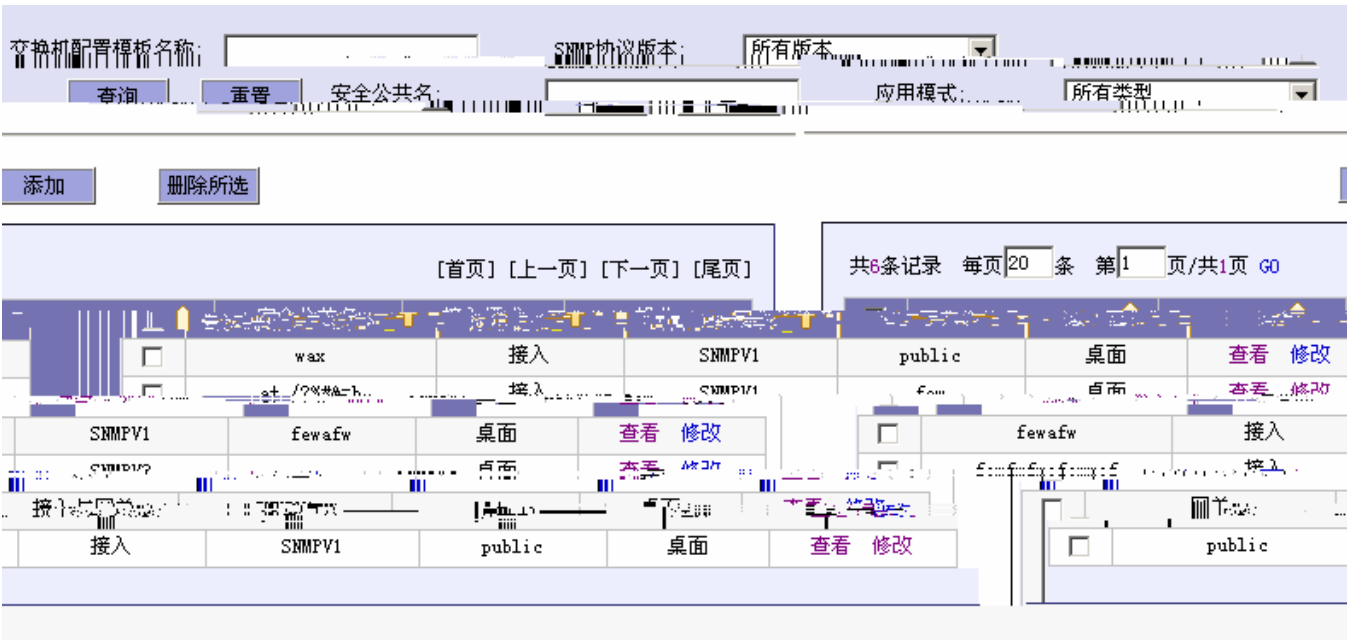
“*”

2.7.2.4

“ ” “ ” “ ” “ ”

2.7.3

2.7.3.1



p “ ” “

p “ ” “ ” “

p “ ” “ ” “

p “ ” “ ” “

2.7.3.2

“ ” “ ” “ ”



-
- 0 ☐
 - 0 ☐
 - 0 ☐
 - 0 ☐
 - 0 ☐

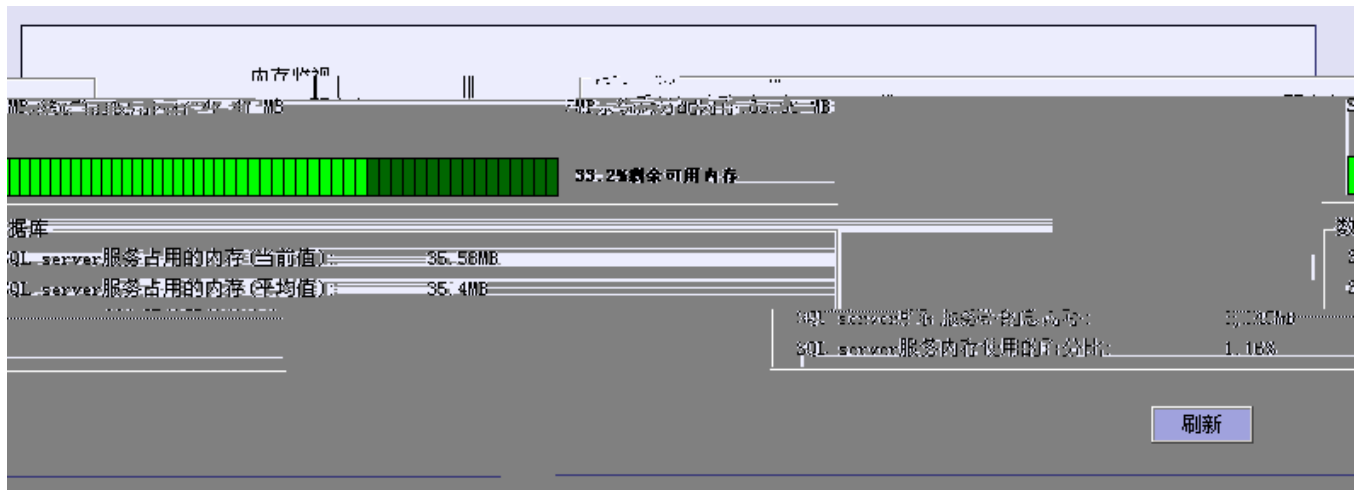
2.8.1

- x
- x SMP SQL Server
- x
- x

 说明

0

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

- o
- o

2.9.1

- ×
 - ×
- SAM

IP SMP

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:

192.168.6.187

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:

60

分钟 (默认为60分钟)

* 配置文件更新服务器:

ftp://smp:smp@192.168.6.137

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 <= 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

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:

120

分钟 (默认为120分钟)

* 访问控制策略同步周期:

60

分钟 (默认为60分钟)

* 修复服务器:

ftp://127.0.0.1/

修改

重置

2.10

SMP

- o
- o

2.10.1

SMP

x “ ”

x “ ”

x “ ”

x “ ” SMP

x “ ”

x “ ”

x

x

x SMP “system”

x

 说明

o

2.10.2

2.10.2.1

“ ” “ ”

日志类型：

所有类型

日志内容：

日志的创建时间 (开始):

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

o

2.10.2.2

“ ” “ ”

日志参数配置

☒ 自动删除 (1~360)*

天以前的端点防护日志

☒ 自动删除 (1~360)*

天以前的安全日志

☒ 自动删除 (1~360)*

天以前的操作日志

☒ 自动删除 (1~360)*

天以前的系统日志

☒ 自动删除 (1~360)*

天以前的客户端信息日志

☒ 自动删除 (1~360)*

天以前的敏感资源防护日志

修改

重置

返回

“

”

“

”

“

”

“

”

“

”

“

”



说明

0

2.11.1

×

×

×

×

×

×

×

×

×

×

TOP N

TOP N

TOP

TOP

2.11.2

2.11.2.1

“ ” “ ” “ ” “ ”

“ ” “ ” “ ” “ ”

安全事件报表配置

事件报表配置地址:

建议只保留12个月的安全事件报表。

只保留12个月的安全事件报表。

注: 为减轻数据库的压力,

重置

返回

修改

“ ” “ ” “ ” “ ”

“ ” “ ” “ ” “ ”

开始日期

结束日期

安全事件类型TOP

交换机TOP

2009-07-15

(默认值为10)

(默认值为10)

生成报表

重置

返回

“

”

“

”

“

”

“

”

“

”

说明

o

o

2.11.2.4

“

”

“

”

“

”

“

”

“

”

2009-07-15

2009-07-15

安全事件类型TOP

交换机TOP

2009-07-15

2009-07-15

(默认值为10)

(默认值为10)

生成报表

重置

返回

“

”

“

”

“

”

“ ” “ ”

 说明

o

o

2.11.2.5 ()

“ ” “ ”

“ ” “ ()” “ ()”

* 开始日期:



* 结束日期:



安全事件类型TOP:

(默认值为10)

生成报表

重置

返回

“ ()” ()

“ ”

N

“ ”

“ ” “ ”

 说明

o

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

o

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 111111111

2.

SMP
IP

3.

SMP SMP HTTP HTTPS
“ / ”
HTTP HTTPS

服务器配置

服务器配置项

服务器安装路径：

D:\RG-SMP

HTTP 协议

☒

设置HTTP 端口：

8080

HTTPS协议

☒

设置HTTPS端口：

8443

JVM内存分配池初始容量 (MB)：

256

JVM内存分配池最大容量 (MB)：

512

JVM PermSize初始容量 (MB)：

128

JVM PermSize最大容量 (MB)：

128

数 据 连 接 池 初 始 容 量 (个)：

5

数 据 连 接 池 最 大 容 量 (个)：

50

☒ 操作系统启动时自动启动

取消

确定

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

5. “ ” session
- SMP

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