

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

山

4

4

4

4

4

4

山



4



4

RGOS®

4

RGNOS®

4



4

Red-Giant®

4

Red-Giant 锐捷®

4

山

山

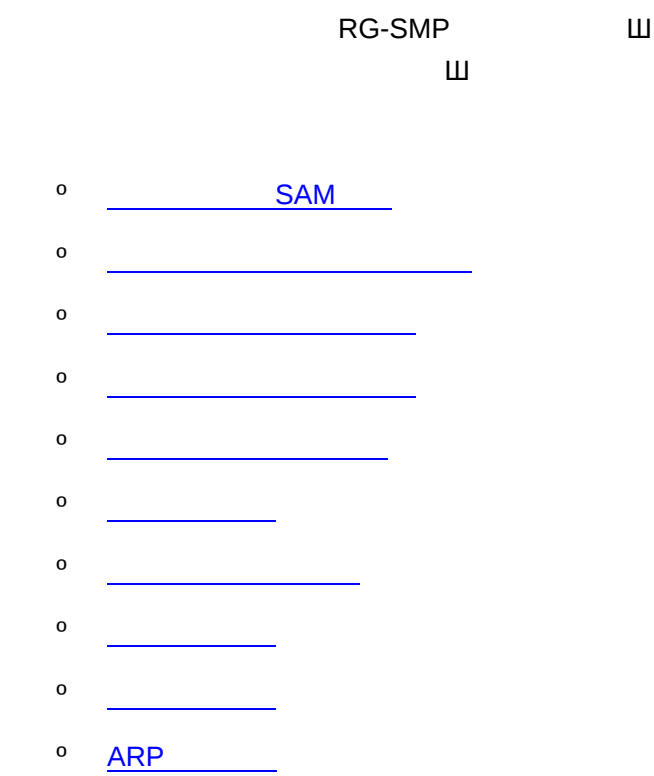
山

4

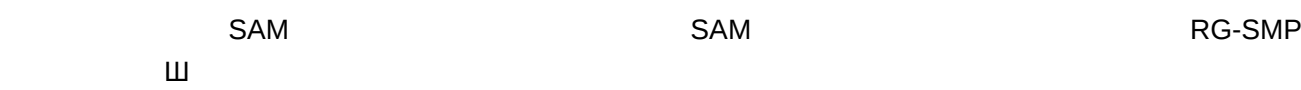
山



1



1.1 SAM



1.1.1



SMP

山

2.

“ ”

山

1.1.3

1.

“ ”

“ ”

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 <= 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:

192.168.6.194

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

* 端点防护状态检测周期:

5

* 软硬件配置信息报告周期:

5

* 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

2.

“ ”

山

8

133

8

1.2

RG-SMP山

1.2.1

[1.1](#)山

1.2.2

1. “ ” “ ”

基本信息

10.0.0.159的权限

限制控制方式

名称	描述	操作
系统		查看
络资源		查看

添加

重置

返回

控制方式

☐ 不控制 ☒ 上网权限

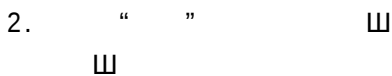
策略列表

☒	上网权限模板
☒	允许访问日志
☒	禁止访问所有网

2. “ ” 山

1.2.3

1. “ ”



RG-SMP PC

1.1 $\mathbb{W}$

1. “ ”
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	自适应顺延天数	7	☒ 查看 修改	江民杀毒软件KV2007及以后的版本	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
支持	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
支持	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
支持	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
支持	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
支持	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
支持	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
支持	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
支持	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

3.

基本信息

杀毒软件名称:

☐ 检查杀毒引擎版本

自适应

☐ 检查病毒库版本

顺延天数:

☐ 版本检查方式:

病毒库自适应原则

注意: 请输入病毒库顺延天数, 它用来限制用户的病毒库最长可以不更新的天数

行内存扫描

☒ 上报不能清除的病毒信息

☒ 认证后立即执行

☒ 全盘扫描时间间隔: 天

☒ 上报未全盘扫描的用户信息

☒ 启用全盘扫描

☒ 网页监视

☒ 邮件监视

☒ 即时通信监视

程序URL:

验证地址

实时提示信息:

病毒库升级:

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

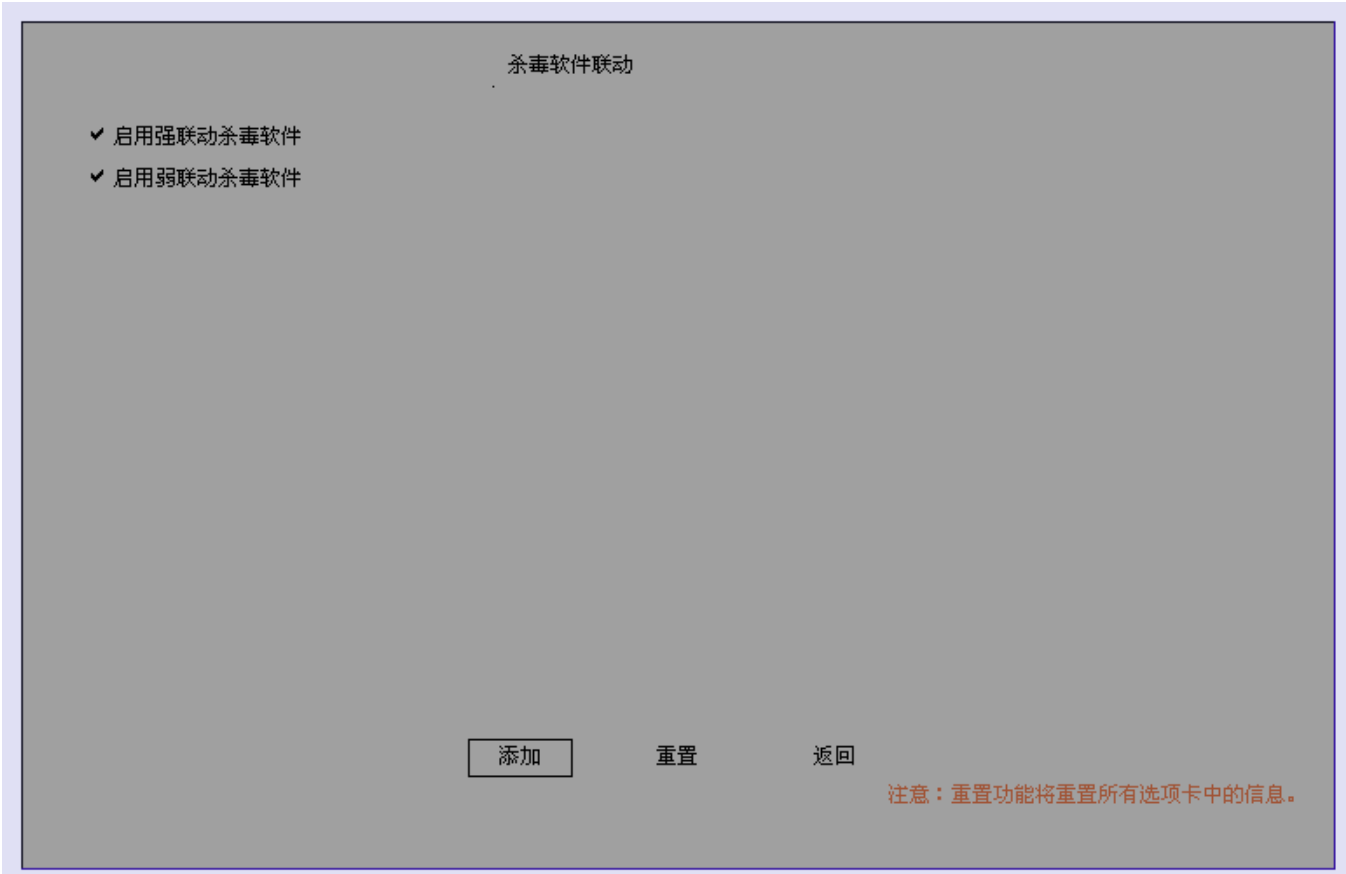
☒ 杀毒软件不合格

☒ 杀毒引擎及病毒库

4. “ ” 山

1.3.3

1.



2. “ ” 山

1.3.4

1. “ ” “ ”

4.

“ ” “ ” “ ”
ftp://[]:[]@[SMP IP]

FTP

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, 你可通过“系统日志”或“系统日志”查看系统日志。

分钟 (默认为60分钟)

/smp:smp@192.168.6.194

客户端配置文件

* 配置文件更新周期: 5

* 配置文件更新服务器: ftp://

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

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)

* 硬件配置信息报告周期: 5 分钟 (默认为5分钟)

分钟 (默认为60分钟)

* 访问控制策略同步周期: 5

* 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ht

修改 重置

5.

“ ” 山

6.

山

1.4

PC

RG-SMP

山

1.4.1

1.1

山

1.4.2

1. “ ”

指定更新服务器

☒ 启用微软补丁更新

更新服务器设置

更新服务器类型：不

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

☒ 定义更新

☒ 关键更新程序

☐ Feature Pack

☐ 必须安装的补丁安全级别：

☐ 全部更新

☒ 紧急

☒ 重要

☒ 次要

☐ 临

☐ 临

更新周期：16 小时 默认16小时

地址：

http://support.microsoft.com/kb/927891/zh-cn

验证URL

过程采取安全措施。

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（如下警告消息、绑定端点防护模板等）。

更新控制

边更新 ☒ 禁用自动更新

更新立即安装：

启用

更新：

自动下载并计划安装

计划安装时间：

10:00

重置

返回

添加

注意：重置功能将重置所有选项卡中的信息。

2. “ ”

山

16

133

16

1.4.3

[1.3.4](#) 山

1.4.4

[1.3.5](#) 山

1.5

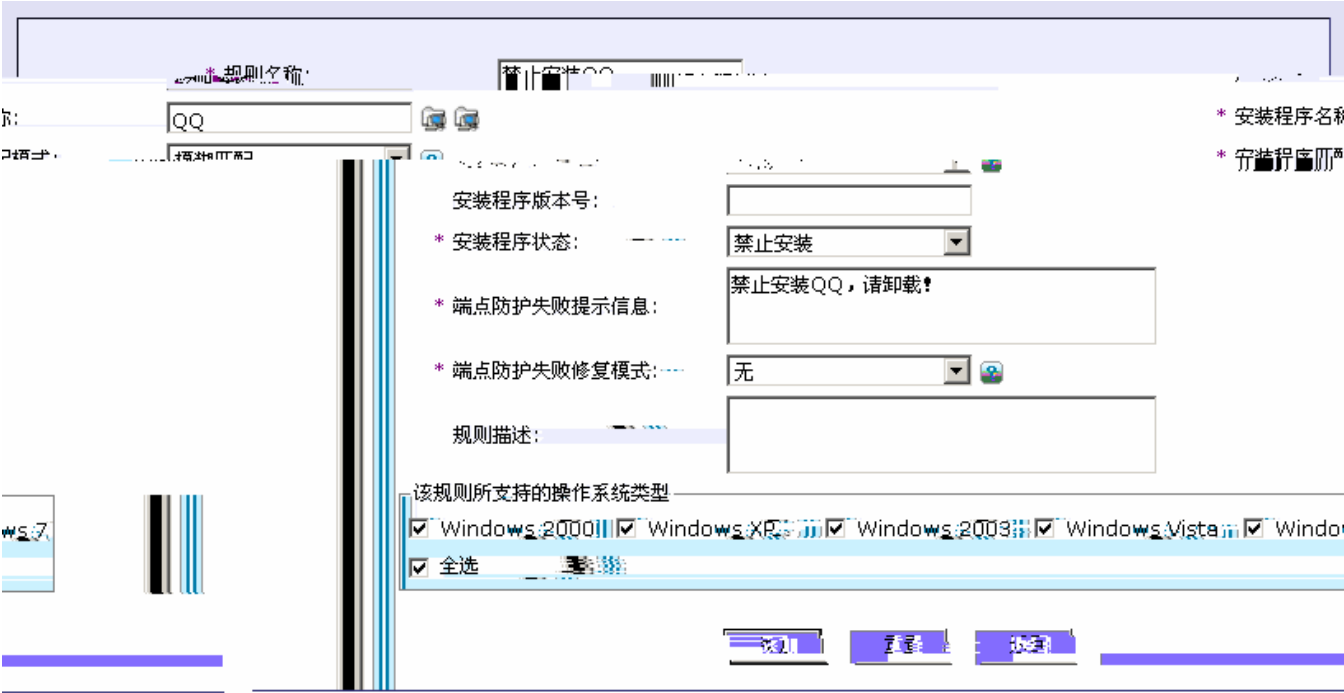
山 RG-SMP PC / / /

1.5.1

[1.1](#) 山

1.5.2

1. “ ” 山
2. “ ”



3. “ ”

* 规则名称: 禁止启动BQQ

* 进程名称: RTX

* 启动方式(默认启动方式): 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

4.

* 规则名称: 强制开启windows防火墙

* 注册表分支名称: HKEY_LOCAL_MACHINE\System\Current ControlSet\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, 为了您能够更好的访问网络, 请开启w... 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

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。

修改 重置 返回

5.

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

4. “ ” 山

1.5.4

1. “ ” > “ ”

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。



2. “ ” Ш

1.5.5

[1.3.4](#) Ш

1.5.6

[1.3.5](#) Ш

1.6

		RG-SMP						PC	
Ш	RG-SMP	PCMCIA	Ч	Ч	Ч	Ч	Ч	Ч	Ч
Ч	U	Ш							

1.6.1

[1.1](#) Ш

1.6.2

1. “ >

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

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！
U盘	强制禁用	禁止使用U盘！

加

重置

返回

添

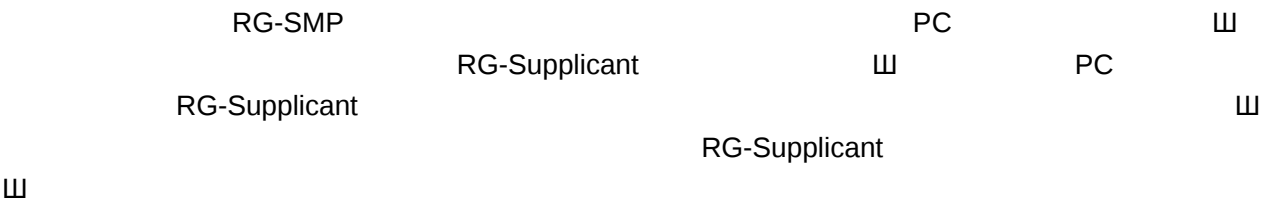
注意：重置功能将重置所有选项卡中的信息。

2. “ ”

1.6.3

[1.3.5](#)

1.7



1.7.1

[1.1](#)

1.7.2

1. “ ” “ ”



2. “ ”

1.7.3

[1.3.5](#)

1.8

RG-SMP RG-SEP

1.8.1

[1.1](#)

1.8.2 RG-SEP

1. “ ” “ ” 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, 192.168.2.23”。配置成功后, 你可通过“系统自诊断”通过端口诊断该服务器与SAM服务器的连接是否正常。

分钟 (默认为60分钟)

/smp:smp@192.168.6.194

正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。

客户端配置文件

* 配置文件更新周期:

5

* 配置文件更新服务器:

ftp://

配置文件更新服务器是指存放锐捷安全认证文件的服务器。

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 <=

60

* 可信度 <=

80

☒ 按可信度过滤对敏感资源的安全事件

* 可信度 <=

60

* 可信度 <=

80

按可信度过滤对敏感资源的安全事件

* 可信度 <=

80

安全事件解析器IP

192.168.6.187

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)

* 该网控制策略报告周期:

5

分钟 (默认为120分钟)

* 修复服务器:

http://192.168.6.187

修复服务器是指存放修复补丁的服务器地址, 必须以http://, https://开头。

重置

修改

2. “ ” 山

1.8.3

1. “ ”



2. “ ” 山

1.8.4

[1.3.5](#) 山

1.9

RG-SMP 山

[1.8](#) 山

1. “ ” > “ ”

基本信息

* 敏感资源IP:

192.168.203.54

* 子网掩码:

255.255.255.255

?

敏感资源名称:

重要服务器

敏感资源描述:

处理模式:

☐ 标准处理模式

☒ 强制下线处理模式

详细处理方式

* 强制下线原因:

你的电脑已中毒，请查杀。

添加

重置

返回

2. “ ”

1.10 ARP

ARP ARP RG-SMP

1.10.1

1. “ ”

* 交换机配置模板名称:

RG_网关

* 应用模式:

网关

* SNMP协议版本:

SNMPV1

?

* 安全公共名:

public

?

添加

重置

返回

2. “ ”

1.10.2

1. “ ”

IP

“

”

SMP

* 交换机IP:

192.168.203.1

* 是否VRRP部署模式:

否

* 交换机配置模板:

RG_网关

* 交换机MAC:

00D0F8BC9511

交换机名称:

交换机类型:

未选择

交换机位置:

备注:

● 如果交换机IP是VRRP部署模式下的虚拟IP, 请配置为VRRP部署模式, 这时候获取交换机信息时, 才能获取

配置模板来绑定安全策略

● 您添加上的用品将自动应用交换机配置模板绑定的安全策略模板。只有当交换机

获取交换机信息

添加

重置

返回

 注意

IP 4

SNMP

SMP

山

2.

“

”

山

1.10.3 ARP

1.

“

> ARP

”

“

ARP

”

“

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
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

2. “ 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
192.168.203.90	00D0F8BC9556	GSN	S2126G	接入与网关	☒	☐	查看

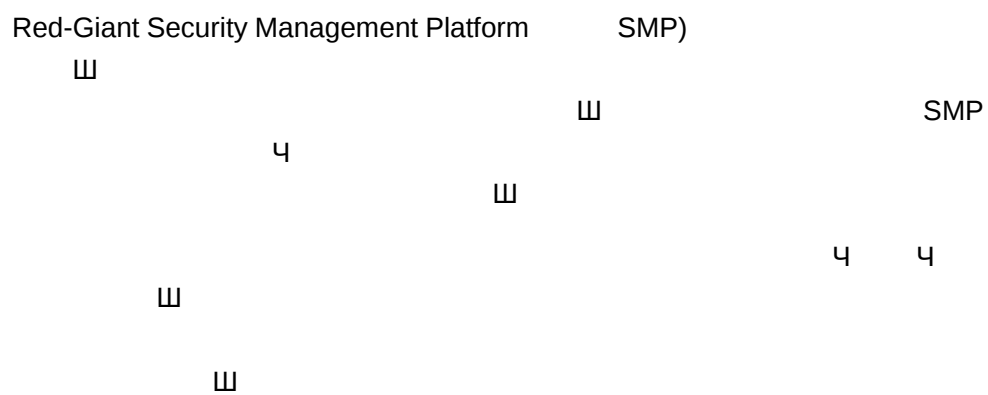
说明

o “ ARP ” ARP 山

o “ ARP ” ARP ARP 山



2



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

2.1



2.1.1

SMP		4	Ш	
×	-----	ШSMP		supervisor
	ruijiesmp Ш			
×	-----	ШSMP		log
	11111111 Ш			
×	-----	SMP		4
	ШSMP		admin	11111111 Ш

2.1.2

SMP		Ш	
×	supervisor	ruijiesmp Ш	
×	log	11111111 Ш	
×	admin	11111111 Ш	



 注意



山

2.1.3

1. “ ” “ ” 山



2. “ ” 山

3. “ ” 山

4. “ ” 山

2.1.4

“ ” 山



2.1.5

4 4 4 山
supervisor 山

2.1.5.1

1. “ ” “ ” 山

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

2. “ ” “ ” “ ”
- ”
- 山
3. “ ” “ ” 山
4.
- p “ ” “ ” 山 “ ”
- 山
- p “ ” 山 “ ”
- 山
- p 山
- p “ ” “ ” 山 “ ”

说明

山

2.1.5.2

1. “ ” “ ” “ ” “ ” 山

* 用户名：

* 所属用户组：

未选择

* 密码：

* 密码确认：

真实姓名：

Email地址：

电话号码：

添加

重置

返回

2. “ ” $\mathbb{W}$
3. “ ” “ ” $\mathbb{W}$
4. “ ” $\mathbb{W}$
5. “ ” “ ” $\mathbb{W}$

 说明

- | | | | | |
|---|-------------|---|---------|-----|
| 0 | | 4 | | 11 |
| 0 | "*" | 4 | 4 | |
| | SUPERVISOR(|) | system(|)11 |
| | | | | 9 |

2. “ ”
3. “ ”
4. “ ”
5. “ ”

```

graph TD
    A[0] --> B[9]
    A --> C[20]
    B --> D[supervisor]
    C --> D
  
```

“ ” “ ”

SMP III

-

2.2.1

[illegible]

2.2.2

SMP SAM SMP

4

2.2.2.1

1. " " " " "

2.2.2.3

1.

2.

3.

4.

 说明

O

2.2.2.4

66

"

“

"

W

 说明

O

 说明

o

山

o

山

2.2.2.6

1. “ ” “ ” “ ”
山

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

2. “ ” 山
3. “
4. “
5. “

2.2.3

2.2.3.1

1.

用户组名称:

用户组描述:

安全策略模板:

用户访问权限:

查询

重置

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]

用户访问权限	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	修改

	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	

2.

山

3.

山

4.

p

山

p

山

p

山

p

山

p

山

”山

“



 说明			
o			山

2.2.3.2

1. “ ” “ ” “ ” 山

* 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

2. “ ” 山

3. “ ” “ ” “ ” 山

4. “ ” 山

5. “ ” “ ” 山

 说明			
o	“*”	32	16 山
o			山

2.2.3.3

1. “ ” “ ” “ ” 山

* 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

2. “ ”
3. “ ” “ ” “ ”
4. “ ”
5. “ ” “ ” “ ”

 说明

- 0 $\frac{1}{2}$ 1
- 0 $\frac{1}{2}$ 1

2.2.3.4

- “ ” “ ”

 说明

- 0 33

2.2.4

SMP 4 4 4 3

2.2.4.1

1. “ ” “ ” “ ”

山

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

2. “ ” “ ” “ ”

山

3. “ ” “ ” 山

4.

p “ ” “ ” 山 “

_____”山

p “ ” 山 “

_____”山

p 山

p “ ” “ ” 山 “

_____”山

2.2.4.2

1. “ ” “ ” “ ” 山

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

2. “ ” 山
3. “ ” “ ” “ ” 山
4. “ ” 山
5. “ ” “ ” 山

说明

o “*”

32

16

山

o

山

o “ ”

山

o “ ”

山

o “ ”

山

2.2.4.3

1. “ ” “ ” “ ” ” 山

基本信息

用户访问权限名称: 普通员工访问权限.....

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

2. “ ” 山
3. “ ” “ ” “ ”
- 山
4. “ ” 山
5. “ ” “ ” 山

 说明

- o 山
- o 山

2.2.4.4

“ ” “ ” 山

 说明

- o 山
- o 山
- 山

2.2.5

SMP 4 4 4 4 山

2.2.5.1

1. “ ” “ ” “ ” 山

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

2. “ ” “ ” “ ” “ ” 山

3. “ ” “ ” “ ” 山

4. “ ” 山

5. p “ ” “ ” 山 “ ” 山
p “ ” 山 “ ” 山
p “ ” “ ” “ ” 山
p “ ” “ ” “ ” 山

2.2.5.2

1. “ ” “ ” “ ” “ ” 山

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

名称:

描述:

* 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。

2. “ ” 山

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:

	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:

添加

重置

返回

注意：重置功能将重置所有选项卡中的信息。

3.

“ ”

山

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。

4.

“ ”



6. “ ” “ ” “ ” 山
7. “ ” 山
8. “ ” “ ” 山

说明

- o “*”

32

16

山
- o

山
- o

山
- o

“ ”
- 山
- o

“ ”

山

“ ”
- o

山
- o

山



o	山
---	---

2.2.5.3

1. “ ” “ ” “ ” 山



2. “ ” 山

3. “ ” “ ” “ ”

山

4. “ ” 山

5. “ ” “ ” 山

说明	
o	山
o	4 4
	“ ”

× 山
 × 山
 × 4 4 4
 4 4 山
 × 山

2.3.2

SMP 4 4 4 山

2.3.2.1

1. “ ” “ ” “ ” 山



2. “ ” “ ” “ ” “ ” 山

3. “ ” “ ” “ ” 山

4.

p “ ” “ ” 山

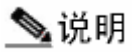
“ ” 山

p “ ” 山 “ ”

“ ” 山

p “ ” “ ” 山

p “ ” “ ” 山



o

山

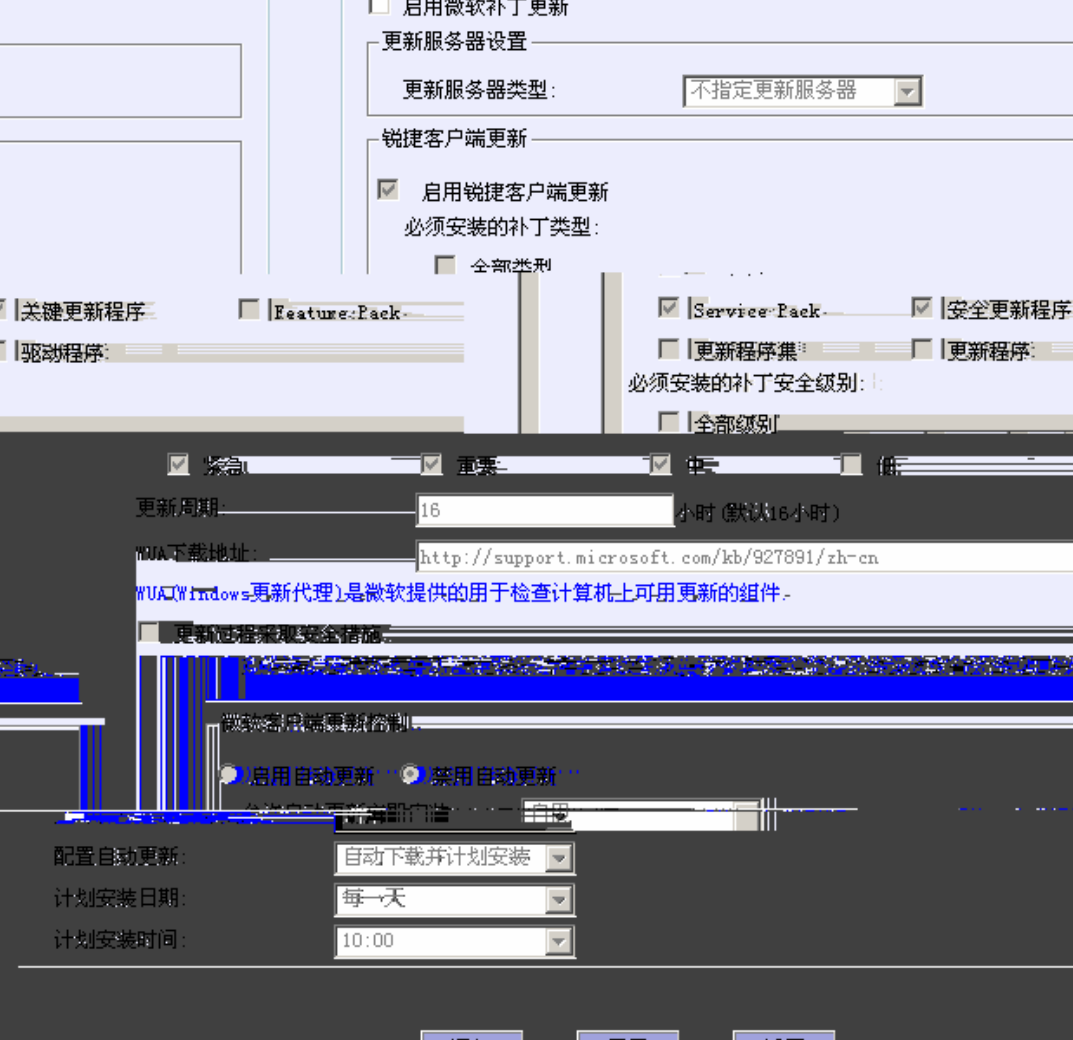
2.3.2.2

1. “ ” “ ” “ ” 山

2. 山

4.

W



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:

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

☒ 关键更新程序 ☐ Feature Pack ☒ Service Pack ☒ 安全更新程序 ☒ 定义更新程序集 ☐ 更新程序 ☐ 主程序

必须安装的补丁安全级别: ☐ 全部级别

☒ 紧急 ☒ 重要 ☒ 中 ☐ 低 ☐ 其他

更新周期: 小时 (默认16小时)

WUA下载地址: [验证URL](#)

WUA(Windows更新代理)是微软提供的用于检查计算机上可用更新的组件。

更新过程采取安全措施。

锐捷客户端更新控制

☐ 启用自动更新 ☒ 禁用自动更新

配置自动更新:

计划安装日期:

计划安装时间:

“ ”

5.

“ ”

” ”

“

"

“

6.

“ ”

W

7.

“ ”

“

"

W

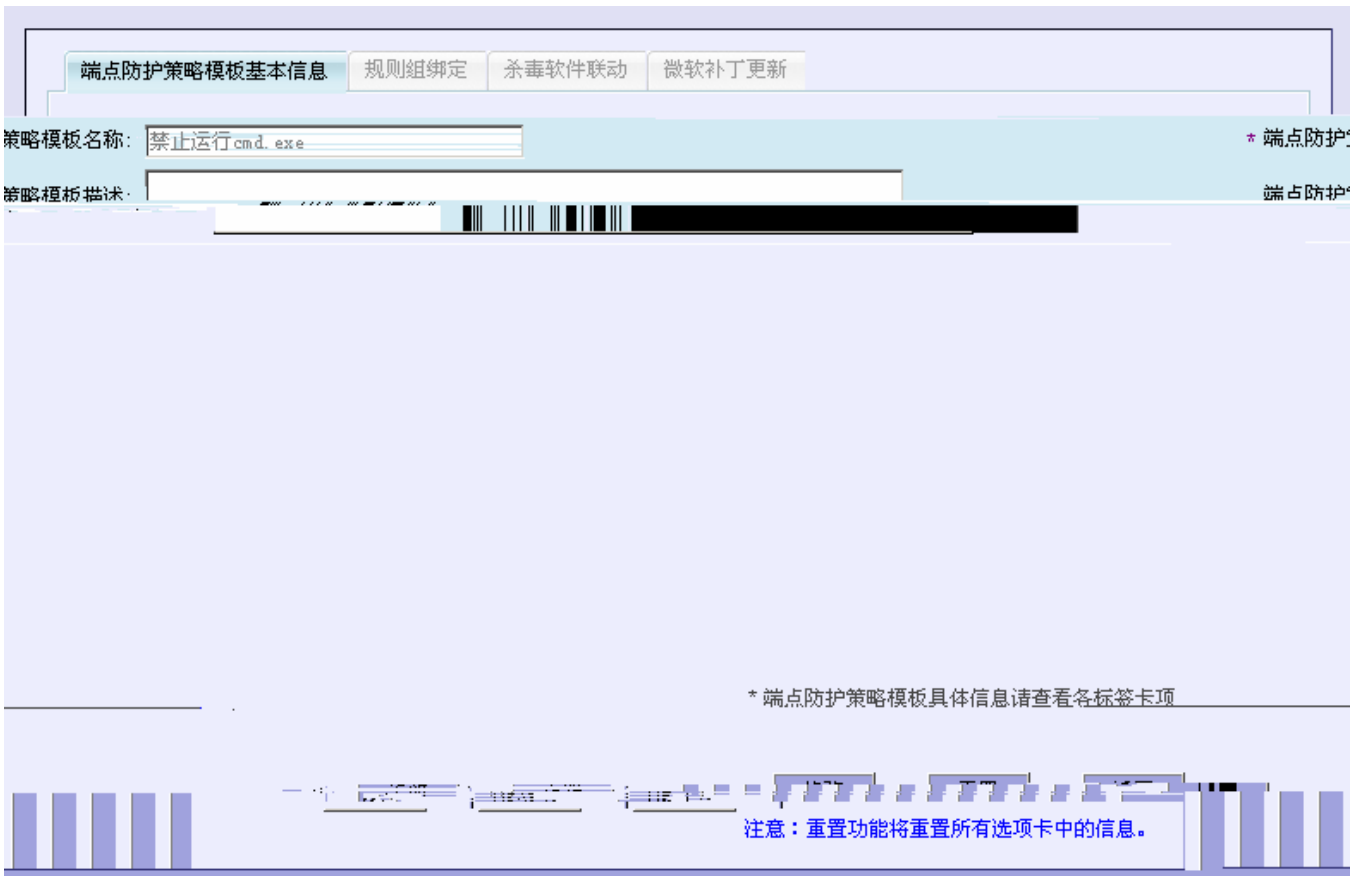


说明

o	“*”	32	16	山
o		山		
o		山		

2.3.2.3

1. “ ” “ ” “ ”



2. “ ” 山
3. “ ” “ ” “ ”
4. “ ” 山
5. “ ” “ ” 山

说明



o	山
o	山

2.3.2.4

“	”	“	”
山			
 说明			
o	山		

2.3.2.5

 说明			
o	“	”	
	山		
o			山
o	“	”	
	(	4	)山
o	WUA(Windows	)	WUA
	山		
o		山	
o	Windows		
o			



		Ш
--	--	---

Ш

Ч



2.3.3.1

1. “ ” “ ” “ ”

Ш



2.

Ш

3.

p

“

”

“

”

Ш

“

_____”Ш

2.3.3.2

1.

“

”

“

”

“

”

Ш

æ

基本信息

杀毒软件名称

卡巴斯基反病毒软件6.0.10.100

病毒库版本

4.0.10.100

病毒库更新方式

自动

病毒库自适应顺延天数

7

病毒库更新地址

http://www.kaspersky.com/updates

验证地址

http://www.kaspersky.com/updates

验证地址

http://www.kaspersky.com/updates

检查病毒库版本

病毒库更新方式

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

病毒库更新地址

验证地址

验证地址

修改

重置

返回

3. “ ” 山
4. “ ” “ ” “ ” 山
5. “ ” 山
6. “ ” “ ” 山

说明

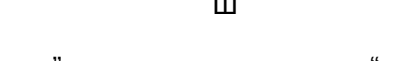
- o 山
- o “ ” “ ” “ ” 山

2.3.4

SMP 4 4 4 山

2.3.4.1

1. “ ” “ ” “ ” “ ” “ ” 山

2. 

3. 

4. 

0 III

1. “ ” “ ” “ ” W

2.3.4.3

1. “ ” “ ” “ ” 三

* 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:	
修改 重置 返回	

2. “ ” 卅

3. “ ” “ ” “ ”

Ш

4. “ ” 卅

5. “ ” “ ” W

 说明

0 III

2.3.4.4

“ ” “ ”

 说明

o

山

2.3.4.5

1. “ ” “ ” “ ” 山

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. “ ” 山

3. “ ” “ ” “ ”

山

4. “ ” 山

5. “ ” “ ” 山

2.3.5

SMP 4 4 4 4 4 4 山

2.3.5.1

1. “ ” “ ” “ ” “ ” “ ”

山

2. “ ” Ⅲ
3. “ ” “ ” “ ” Ⅲ
4. “ ” Ⅲ
5. “ ” “ ” Ⅲ

1. " " " " " W

* 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

2. “ ” 山
3. “ ” “ ” 山
4. “ ” 山
5. “ ” “ ” 山

说明

- o “*”

128

64

山
- o

山
- o

“ ”山
- 山
- o

“
- ”山

山
- o

“ ”

山

1. “ ” “ ” “ ”

2. “ ” W
3. “ ” “ ” “ ” W
4. “ ” W
5. “ ” “ ” W

“*”	128	64	W
		W	
W			W

2.3.5.6

1. “ ” “ ” “ ” 山
2. “ ” 山
3. “ ” “ ” “ ” 山
4. “ ” 山
5. “ ” “ ” 山

 说明

0 山

2.3.5.7

“ ” “ ” 山

 说明

0 山

2.3.5.8

1. “ ” “ ” “ ” “ ” “ ” 山

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

2. “ ...”

3.

“ ”

山
4.

“ ”

山
5.

“ ”

“ ”

山

说明

- 0

10M

山
- 0

SMP

“ ”

“ ”

山
- 0

“ ”

“ ”

山

2.3.5.9

1.

“ ”

“ ”

“ ”

“ ”

“ ”

“ ”

“ ”

山

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

2.

“ ”

“ ”

“ ”

山
3.

“ ”

山
4.

“ ”

山
5.

“ ”

“ ”

山
6.

“ ”

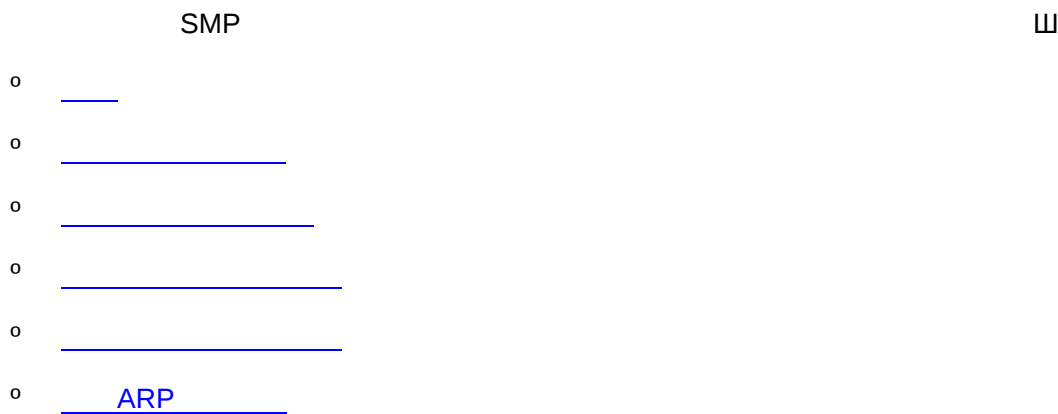
山

说明

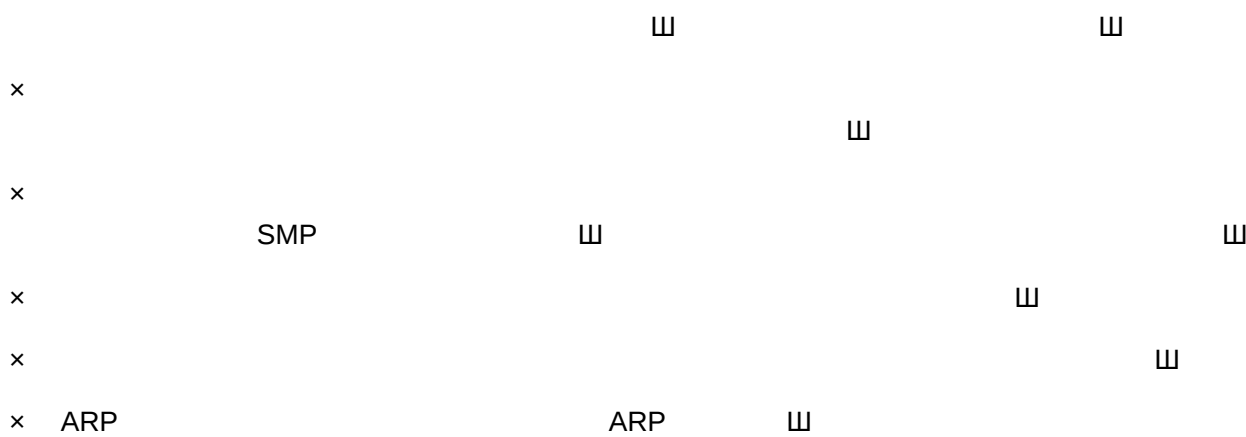


o	Ш	
o	.dat	Ш

2.4



2.4.1



2.4.2

SMP 4 4 4 4 Ш

2.4.2.1

1. “ ” “ ” “ ” Ш



2. 
3. 
4. 

0 $\frac{1}{3}$ $\frac{2}{3}$ 1

2.4.2.2

1. " " " " " " W

基本信息

*

IP地址

*

子网掩码

255.255.255.255

?

网关地址

模板名称

?

☒ 模板内网模式

☐ 模板内网外网模式

*

模板

?

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

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

添加

重置

返回

2. “ ” 山
3. “ ” “ ” “ ” 山
4. “ ” 山
5. “ ” “ ” 山

说明

“*”

山

山

山

山

“ ”

山

“ ”

2.4.2.3

1.

2.4.3.1

1. " " " " "

III

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					
导出安全事件类型 导出安全措施 导出查询出的安全措施 删除所选					
共181条记录 每页20条 第159页/共160页 GO [首页] [上一页] [下一页] [尾页] 					
☐	安全事件类型名称	安全等级 ↑	发生次数 ↑	安全措施	操作
☐	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
☐	应用攻击频率处理模式	查看 修改	0	SUNRPC_ttdbserve溢出尝试	严重
☐	应用攻击频率处理模式	查看 修改	0	TMail_Delete_命令挂出利用	严重
☐	UDP_rpc.xfsmd_xfs_export尝试	通知	0	应用攻击频率处理模式	查看 修改
☐	B_RPCSS_拒绝服务	重要	0	应用攻击频率处理模式	查看 修改
☐	TCP_ypupdated进程请求	通知	0	应用攻击频率处理模式	查看 修改
☐	TCP_rwalla进程请求	通知	0	应用攻击频率处理模式	查看 修改
☐	ypserv.man.list_请求(TCP)	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	查看 修改

2. “ ” “ ”

III

3. " " " "

111

4. “ ”

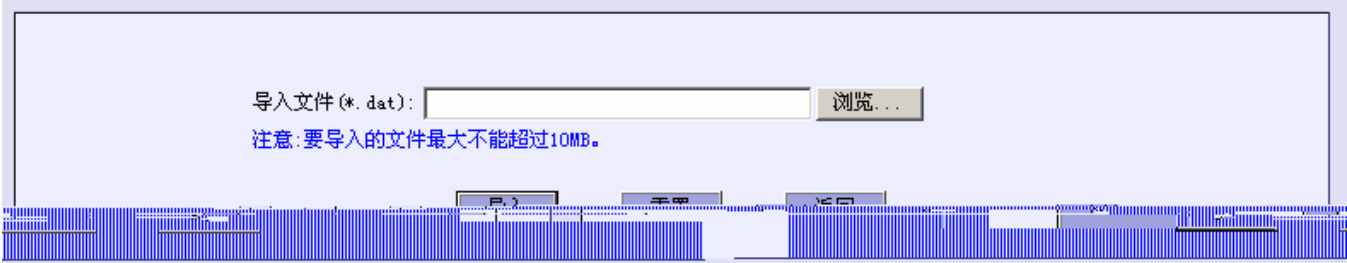
111

b “ ” III

“ ”

2.4.3.3

1. “ ” “ ” “ ”



- 2. “ ...”
- 3. “ ”
- 4. “ ”
- 5. “ ” “ ”

 说明

- o 10M
- o SMP “ ” 4 4 4
- o

2.4.3.4

- 1. “ ” “ ”
- 2.

 说明

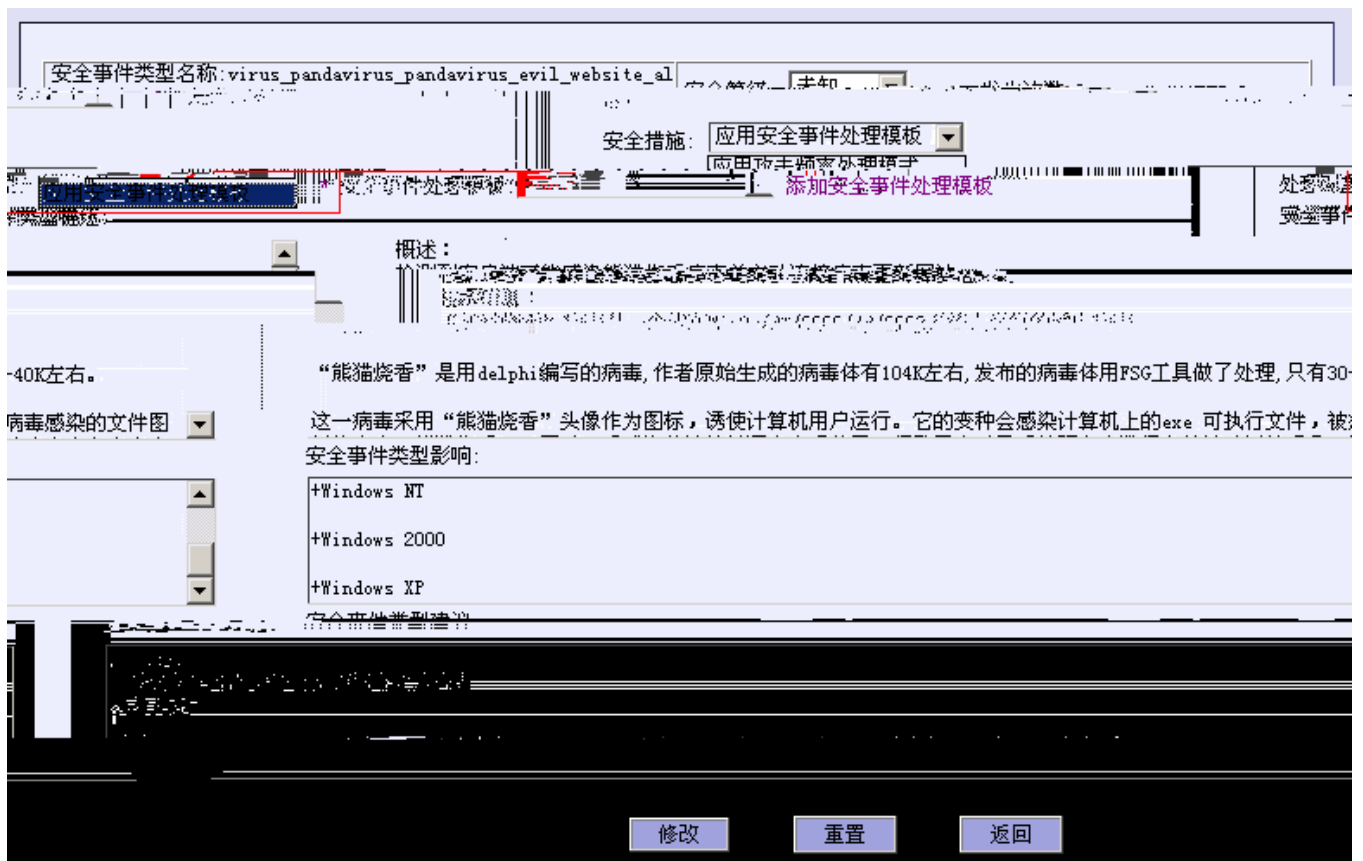
.dat

2.4.3.5

1. " " " " " "

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”是周知编写的一种病毒,它来源于做成的病毒文件,它的病毒使用32C语言编写,只读80K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			
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

2. “ ”



3. “ ” 山

“ ”山

4. “ ” “ ”

“ ” 山

5. “ ” 山

6. “ ” “ ” 山

说明

o 山

o “ ”

山

o “ ” “ ”

山

2.4.3.6

1.

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”病毒是一个能在 Windows 9X/2000/XP/2003 系统上运行的蠕虫病毒。 “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			
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

2. “ ” 卅

3. “ “ “ “ ”

“ ” III

4. “ ” III

5. “ ” “ ” W

⚠ 注意

0 11



2.4.3.7

“

”

“

”

山

 说明

o

2.4.5.1

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.

3.

4.

p

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:

☐	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

2. “ ” 山
3. “ ” “ ” “ ”
- ” 山
4. “ ” 山
5. “ ” “ ” 山

说明

o 山

2.4.5.4

“ ” “ ” 山

 说明

o

山

2.4.6 ARP

1. “ ” “ARP” “ ARP”
山

☒ 启用ARP欺骗免疫功能

共15条记录 每页1条 第1页 共15页 02

「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	☒

2. “ ” 山
3. “ ARP ” ARP 山
4. “ ARP ” ARP 山
5. “ ARP ” ARP 山

 说明

o

ARP 山

o

“ > ” ARP ARP
山

2.5

SMP

山

o

o

o

o



o



2.5.1

Ш

ч

ч

×

Ш

×

Ш

×

HTTP ч FTP Ш

×

Ш

Ш

[illegible]0 $\frac{1}{3}$ $\frac{2}{3}$ 1

1. " " " " " W

访问控制模板类型：

未选择

访问控制模板：

未选择

访问控制模板组：

未选择

选择在线用户：

交换机端口：

用户IP：

用户MAC：

返回

添加

重置

2.

山
3.

“ ”

“ ”

“ ”

山
4.

“ ”

山
5.

“ ”

“ ”

山

说明

0

“ ”

“ ”

山

“ ”

山

2.5.2.3

1.

“ ”

“ ”

“ ”

山

* 访问控制模板类型：

阻断模板

* 访问控制模板：

阻断

选择在线用户：

交换机IP：

192.168.203.90

交换机端口：

2

用户IP：

用户MAC：

修改

重置

返回

[illegible]

2.5.3.2

1. “ “ “ “ “ ” W

* 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	

2. “ ” 卅

3. “ ” “ ” “ ” 三

4. “ ” 卩

5. “ ” “ ”



* 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

2. “ ” 山
3. “ ” “ ” “ ” 山
4. “ ” 山
5. “ ” “ ” 山

 说明

- o “*” 32 16 山
- o 4 山

2.5.3.4

1. “ ” “ ” “ ” 山

* 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	山
0		4	山	

1. " " " " " W

2. “ ”
3. “ ”
4. “ ”
5. “ ”

95



O	“★”				32		16		山
O				4		山			
O		“	”	“	”			山	
O	“		”						
		山							
	山								

2.5.3.6

1. “ ” “ ” 山
2. “ ” 山
3. “ ” “ ” “ ” 山
4. “ ” 山
5. “ ” “ ” 山

说明

O			山						
O					山				
O								“	
	”	“		”	“	”	山		
		“		”	山				

2.5.3.7

“ ” “ ” 山

说明

O					山				
---	--	--	--	--	---	--	--	--	--

2.5.4

SMP 4 4 4 4 山

2.5.4.1

1. “ ” “ ” “ ” 山

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

2. “ ” “ ” “ ” “ ” 山

3. “ ” “ ” “ ” 山

4. p “ ” “ ” 山
“ ” 山
p “ ” 山 “ ”
“ ” 山
p 山
p “ ” “ ” 山
“ ” 山

说明

o 山

2.5.4.2

1. " " " " " " W

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
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	☐ 禁止

添加

重置

返回

2. “ ” 卅

3. “ ” 三

4. “ ” III

5. " " " " III

 说明

- | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 |
|---|---|---|---|---|---|---|---|---|---|----|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 |

2.5.4.3

1. “ ” “ ” “ ” “ ”

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

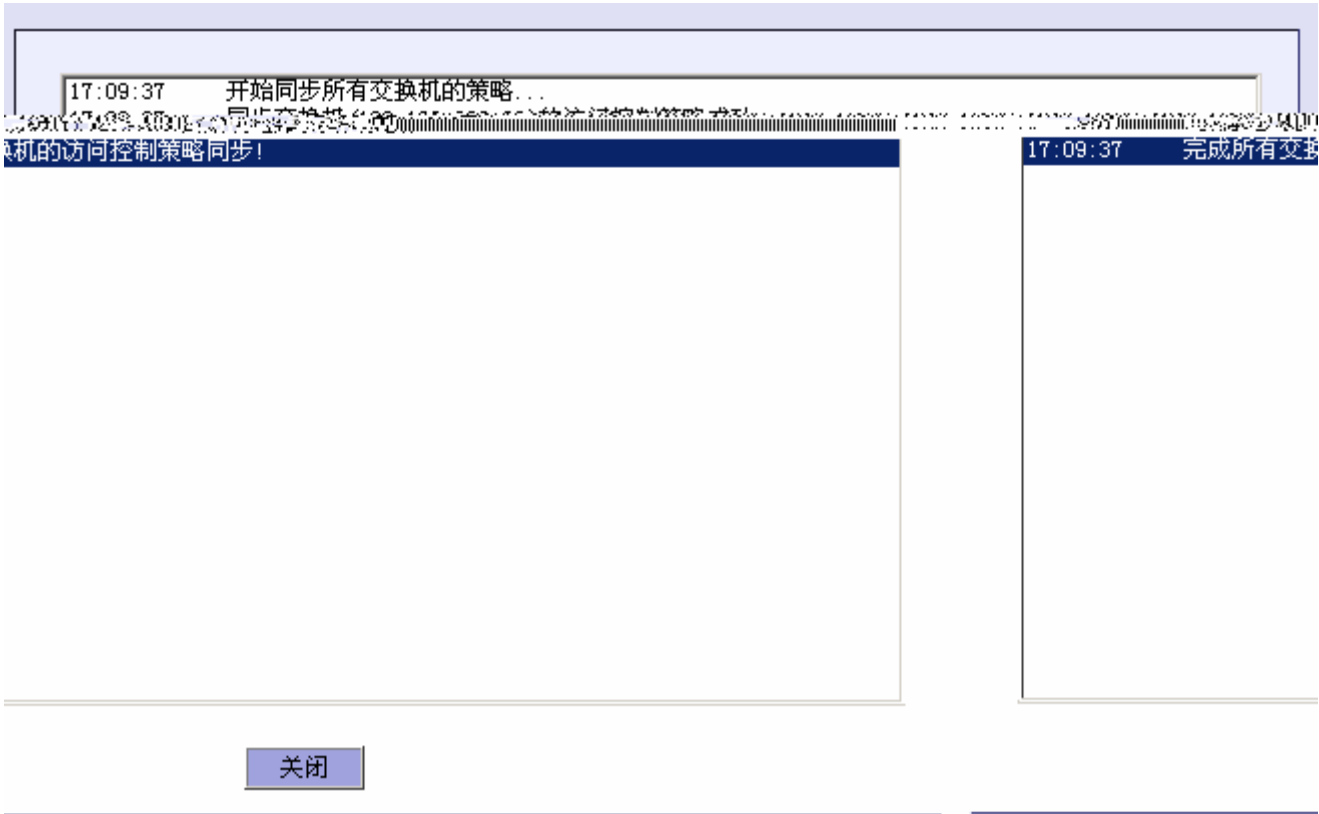
☐	访问控制模板名称	访问控制模板类型	访问控制模板描述	详细信息
☒	隔离到203网段	隔离		查看
☒	禁止访问TELNET服务	阻断	禁止用户访问TELNET服务	查看
☒	禁止访问FTP服务	阻断	禁止用户访问FTP服务	查看
☒	禁止访问SSH服务	阻断	禁止用户访问SSH服务	查看

修改

重置

返回

2.



	说明
o	山

2.6

SMP	山
o	_____
o	_____
o	_____
o	_____

2.6.1

x	山
x	MAC
山	山



×

Ш

Ш

×

Ш

×

Ш

2.6.2

4 Ш

2.6.2.1

1. “ ” “ ” “ ”

” Ш

主机MAC地址:

应用程序名称:

删除所选

删除全部查询结果

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]

详细信息

关联在线用户 查看

☐	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

2. “ ” ” “ ” “ ”

” Ш

3. “ ” “ ” Ш

4.

p “ ” Ш “ _____

” Ш

p “ ” Ш “ _____

_____” Ш

p Ш

p “ ” “ ”

Ш



2.6.2.2

1. “ ” “ ” “ ” Ш

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	名称	应用程序名称	应用程序版本	应用程序名称	应用程序版本
the Ethernet developer community, http://www.ethereal.com	Broadcom	Broadcom 440x 10/100 Integrated Controller	0.10.12	Ethernet 0.10.12	0.10.12
Sun Microsystems, Inc.	Intel(R) Extreme Graphics Driver	Intel(R) Extreme Graphics Driver	1.5.0.50	Intel(R) Extreme Graphics Driver	1.5.0.50
Update 5	J2SE Runtime Environment 5.0 Update 5	J2SE Runtime Environment 5.0 Update 5	1.5.0.50	J2SE Runtime Environment 5.0 Update 5	1.5.0.50
aplicant v3.90	IDM Computer Solutions, Inc.	IDM Computer Solutions, Inc.	3.1 beta4	Ruijie Super UltraEdit	WinRAR 解压
3.1 beta4	Politecnico di Torino	Politecnico di Torino	一键GHOST 8	一键GHOST 8	一键GHOST 8
文件管理器					
2 Build 050706					



” 卩

4. “ ” 卩

5. “ ” “ ” 卩



”

山

3. “ ” “ ” 山

4.

p “ ” 山 “ ” 山

p “ ” 山 “ ” 山

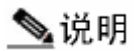
_____” 山

p 山

p “ ” “ ” “ ” 山

p “ ” “ ” 山

p “ ” google 山



o 4

山

2.6.3.2

“ ” “ ” 山

“ ” “ ” 山

2.6.3.3

1. “ ” “ ” “ ” “ ” 山

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. “ ” “ ” “ ” “ ” “ ” 山



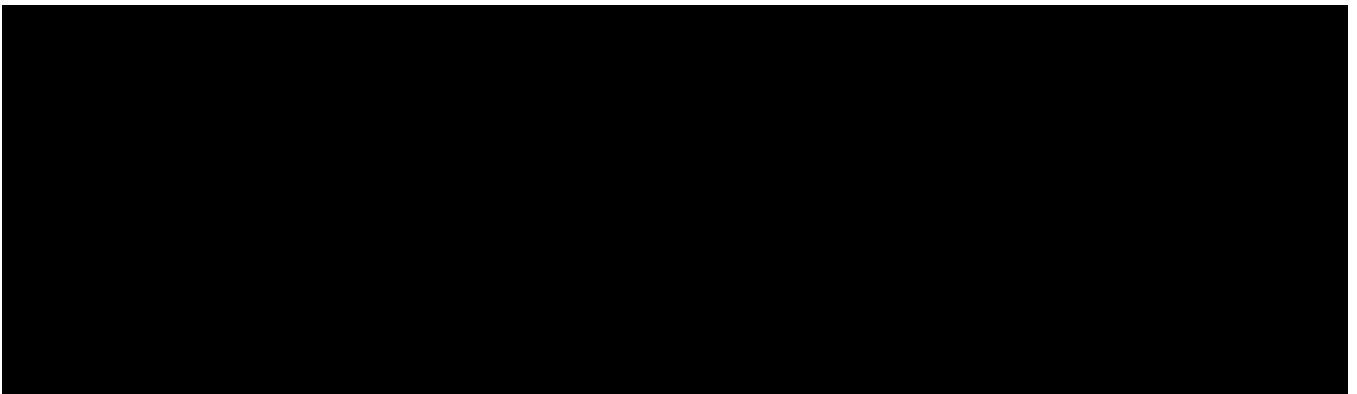
3. “ ” “ ”
Ш
4. “ ” Ш
5. “ ” “ ” Ш

2.6.4

ч ч ч ч ч Ш

2.6.4.1

1. “ ” “ ” “ ”
” Ш



2. “ ” “ ” “ ”
” Ш
3. “ ” “ ” Ш
4.
p “ ” Ш “ ” Ш
p Ш
p “ ” “ ” “ ” “ ” Ш
p “ ” “ ” “ ” “ ” Ш
p “ ” “ ” “ ” Ш
p “ ” “ ” “ ” Ш



 说明

0

山

2.6.4.2

1. “ ” “ ” “ ” 山

* 应用程序分类名称:

应用程序分类描述:

添加

重置

返回

2. “ ” “ ” “ ” “ ” 山

3. “ ” 山

4. “ ” “ ” 山

 说明

0 “*”

山

2.6.4.3

1. “ ” “ ” “ ” “ ” 山

* 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. “ ” “ ” “ ” “ ” 山

3. “ ” 山



4.

“

”

“

”

Ш

2.6.4.5

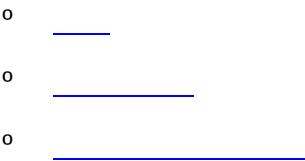
“ ” “ ”

Ш

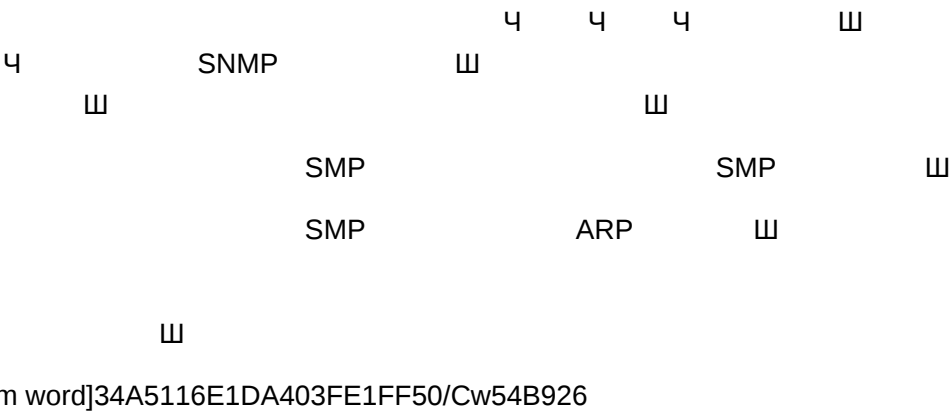
2.7

SMP

Ш



2.7.1



[comm word]34A5116E1DA403FE1FF50/Cw54B926

山

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]

2. “ ” “ ”

山

3. “ ” “ ” 山

4. “ ” “ ”

“ ” 山

5.

p “ ” “ ” “ ” 山

p “ ” “ ” “ ” 山

p “ ” “ ” 山

p “ ” 山

p “ ” MAC” MAC

山

p 山

p “ ” 山

p “ ” “ ” “ ” 山

p “ ” “ ” “ ”

山

2.7.2.2

1. “ ” “ ” “ ” 山

2. “ ” IP 4 “ ”
Ш
3. “ ”
Ш
4. “ ” Ш
5. “ ” “ ” Ш

O “”
 O “” ARP
 ARP “” ARP
 ARP “” ARP

1. " " " " " "

* 开始IP:

* 结束IP:

* 交换机配置模板:

未选择

开始搜索

返回

取消

2. " " 山
3. " " " " 山
4. " " " " 山
- SMP " "

正在搜索，请耐心等待...

1% (搜索到 3 台交换机)

停止搜索

返回

注意：停止搜索功能将中断正在执行的搜索，返回已经搜索到的交换机信息。

5. 山
6. " " " " 山
7. " " " " 山
8. 100 " " " "

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
6	S2652G	public	查看
7	S2628G	public	查看
8	S3760-12SFP	public	查看
9	S2126G	public	查看
10	S2628G	public	查看
11	S8606	public	查看
12	S5760-24GT/4SFP	public	查看
13	S5750S-24GT/12SFP	public	查看
14	my switch	S2652G	查看
15	S5760-24GT/4SFP	public	查看
16	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_780
☐	192.168.203.90	GSN

9. “ ” “ ”
10. “ ” “ ”
11. “ ” “ ”
12. “ ”
13. “ ”

说明

“*”

2.7.2.4

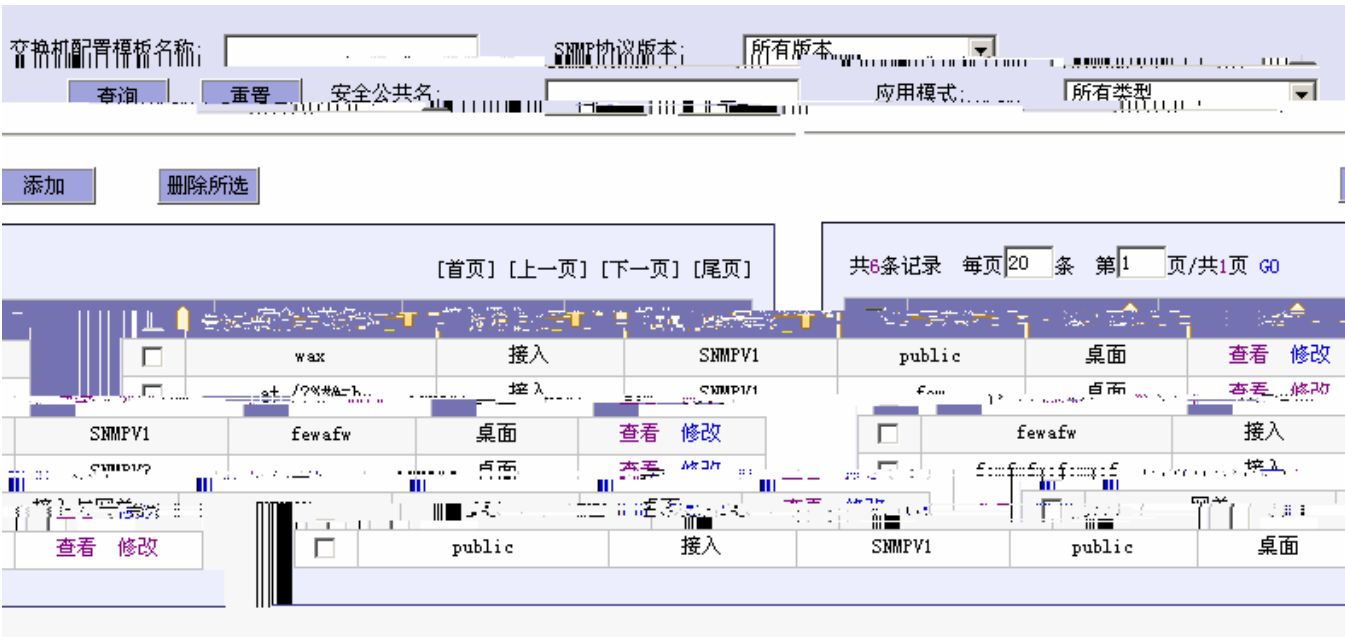
1. “ ” “ ” “ ”

2.7.3

4 4 4 山

2.7.3.1

1. “ ” “ ” “ ” 山



2. “ ” “ ” “ ” 山

3. “ ” “ ” “ ” 山

4. p “ ” “ ” “ ” “ ” 山
”山
p “ ” “ ” “ ” “ ” “ ” 山
p 山
p “ ” “ ” “ ” “ ” “ ” 山

2.7.3.2

1. “ ” “ ” “ ” “ ” “ ” 山

* 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. 本配置模板如果指定安全策略模板,则所有接入上的用户将应用该策略的安全策略模板。但是,如果指定策略模板是空策略模板,则:

2. 如果指定策略模板为空策略模板,则所有接入上的用户将应用该策略的安全策略模板。但是,如果指定策略模板是空策略模板,则:

3. 如果指定策略模板为空策略模板,则所有接入上的用户将应用该策略的安全策略模板。但是,如果指定策略模板是空策略模板,则:

4. 如果指定策略模板为空策略模板,则所有接入上的用户将应用该策略的安全策略模板。但是,如果指定策略模板是空策略模板,则:

添加

重置

返回

2. “ ” “ ”
- “ ” 山
3. “ ” 山
4. “ ” “ ” 山

说明

o “*”	64	32	山
o		山	山
o		山	山

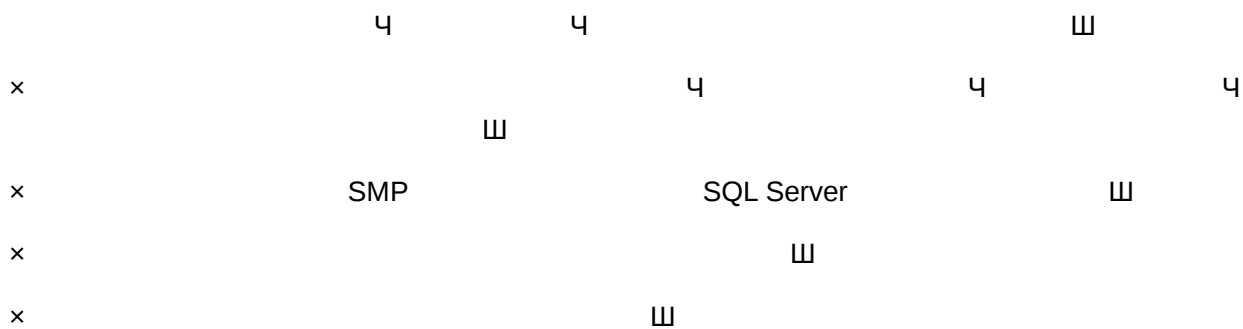
2.7.3.3

1. “ ” “ ” “ ” “ ” 山



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

2.8.1

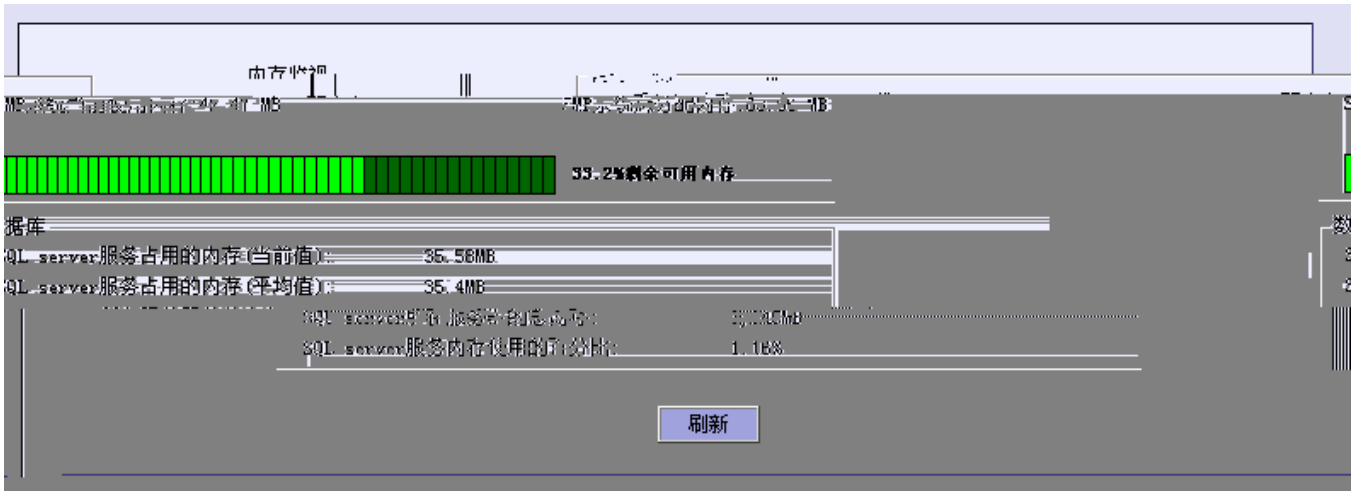


 说明

o _____ 3

2.8.2 - 8 - 2

3 “ ” “ ” “ ” “ ”



2. “ ” 山

2.8.4

1. “ ” “

2.8.5

1. “ ” “ ” “ ”

☒ 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

2. “ ”

3. “Telnet” telnet

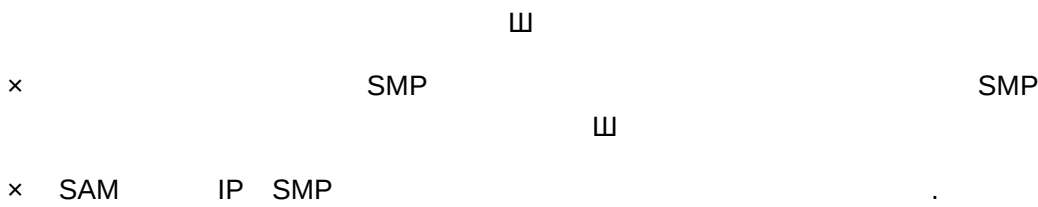
4. “ ” “ ” “ ” “ ” “ ”

5. “ ”

2.9



2.9.1



×

SMP

W

X

X

X

IP SMP
IP

“ ”

127.0.0.1

192.168.1.2

127.0.0.1

X

SMP

WSMP

/ /

9090Ш

×

5 山

×

W

120

W

X

SMP

SMP

SMP

60 山

x

W

2.9.2

1.

“ ” “ ”

SMP

W

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:

192.168.6.181

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:

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. “ ” “ ” 山
3. “ ” “ ” 山

2.10

SMP

山

- o
- o

122

133

122



2.10.1

SMP									
×	“	”					Ш		
×	“	”				Ш			
×	“	”						4	4
			Ш						
×	“	”	SMP				4		Ш
×	“	”				Ш			
×	“	”						Ш	
×									
×									
×			SMP				“system”		
×									

说明

o							Ш		
			Ш						

2.10.2

	4		Ш						
--	---	--	---	--	--	--	--	--	--

2.10.2.1

1.		“	”	“	”				
		Ш							

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
------	------	-------	------

2. “ ” “ ”

山

3. “ ” “ ” 山

4. 山

说明

o 山

2.10.2.2

1. “ ” “ ”

山

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

2. “ ” “ ” “ ”

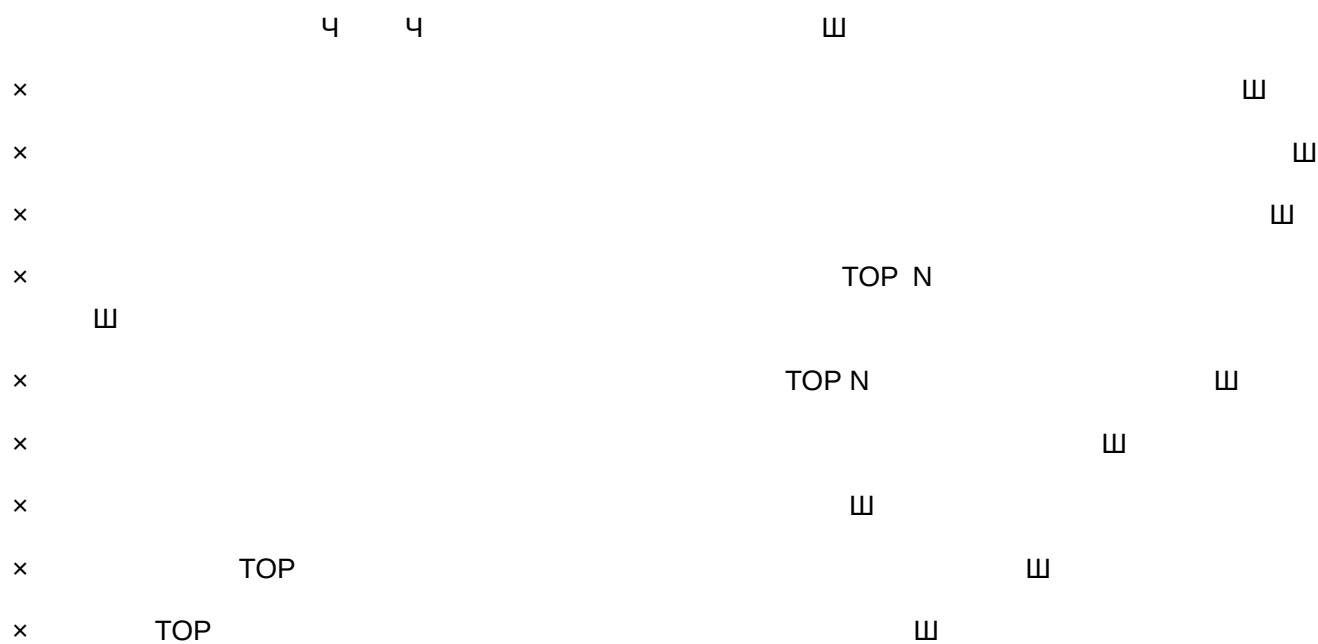
3. “ ” “ ” “ ”

4. “ ” “ ” “ ” “ ” “ ”

 说明

o

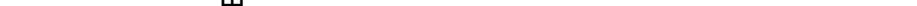
2.11.1



2.11.2



2.11.2.1

1. 
2. 
3. 

安全事件报表配置

默认时间范围: 最近 1 个月

只保留 12 个月的安全事件数据。

建议只保留 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

4. “ ”
- ”
- Ш
5. “ ”
- Ш
6. “ ”



说明

o	12	山
---	----	---

2.11.2.2

1. 山
2. “ ” “ ” 山
3. “ ” “ ” “ ” 山

* 开始月份:

2009 年 07 月

* 结束月份:

2009 年 07 月

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

4. “ ” “ ”
5. “ ” 山
6. “ ” “ ” 山

说明

o	山
o	山

2.11.2.3

1. 山
2. “ ” “ ” 山
3. “ ” “ ” “ ” 山

开始日期:

结束日期:

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

4. “ ” “ ”
- 山
5. “ ” 山
6. “ ” “ ” 山

说明

- o 山 山
- o 山

2.11.2.4

1. 山
2. “ ” “ ” 山
3. “ ” “ ” “ ” 山

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

4. “ ” “ ”
- 山
5. “ ” 山

6. “ ” “ ” 山

 说明

o 山

o 山

2.11.2.5 ()

1. 山

2. “ ” “ ” 山

3. “ ” “ ()” “ ()”
山

* 开始日期:

2009-07-15

* 结束日期:

2009-07-15

安全事件类型TOP:

(默认值为10)

生成报表

重置

返回

4. “ ()” ()
“ ” N
山

5. “ ” 山

6. “ ” “ ” 山

 说明

o 山

2.11.2.6 ()

1. 山



2. “ ” “ ” 山

3. “ ” “ ()” “ ()” 山

* 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

4. “ ()” () “
” È



说明		
0	山	

2.11.2.8

1. “ ” “ ” “ ” 山

此功能用于生成硬件分布情况报表

生成报表

返回

2. “ ” “ ” 山

3. “ ” “ ” 山

3 FAQ

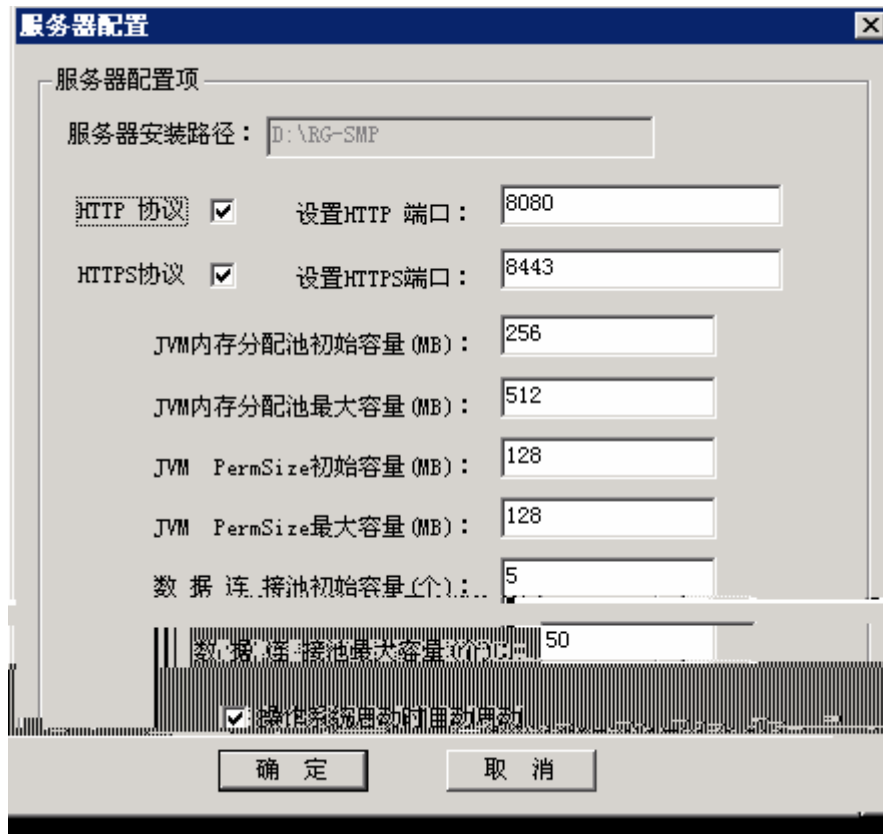
1.

SMPhttp://127.0.0.1:8080/smp/index.jspadmin111111111山
2.

SMPIP 4 4 4 4 山
3.

SMP HTTP HTTPS山

SMP “ / ” HTTP HTTPS 山



4. “ ” session

SMP IE “ ” “ ” Ш

IE SMP Ш

5. “ ” session

SMP Ч Ч Ш

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