RG-IDP

V1.0

©2008

2.

3.

Enter a

a

1+ 2 Ctrl+Alt+A Ctrl

Alt A

..... 3
..... 3
1

6.1.1 39
6.1.2 (Blacklist Configuration) 40
6.1.3 (Device Time Information) 40
6.1.4 (Management Setting) 41
6.2 41
6.2.1 42
6.2.2 42
6.3 43
6.3.1 43
6.3.2 43
6.4 44
6.4.1 44
6.4.2 FTP 44
6.4.3 45
7 46
7.1 46
7.2 VLAN 48
7.3 49
7.4 50
8 .....

9.3 69
9.3.1 69
9.3.2 71
9.3.3 71
9.3.4 72
9.4 / 73
9.5 74
9.5.1 75
9.5.2 76
9.5.3 78
9.6 Botnet 78
9.6.1 79
9.6.2 RBL 80
9.7 81
9.7.1 82
9.7.2 85
9.8 86
9.8.1 < > 86
9.8.2 87
9.8.3 87
9.8.4 88
9.8.5 89

1

RG-IDP

ISMS

Skype Tunnel IM P2P

P2P FTP

BotNet BotNet

RG-IDP 1800

RG-IDP (EABSM) state machine( )

RG-IDP 300+ TCP SYN Flood TCP Flood UDP Flood ICMP Flood TCP Port Scan UDP Port Scan

Botnet

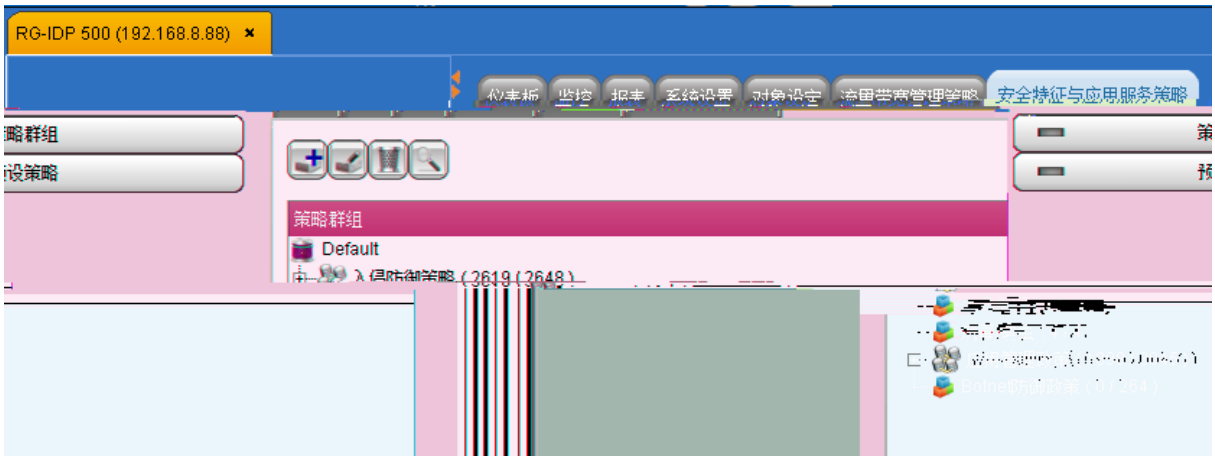
RG-IDP 下

2

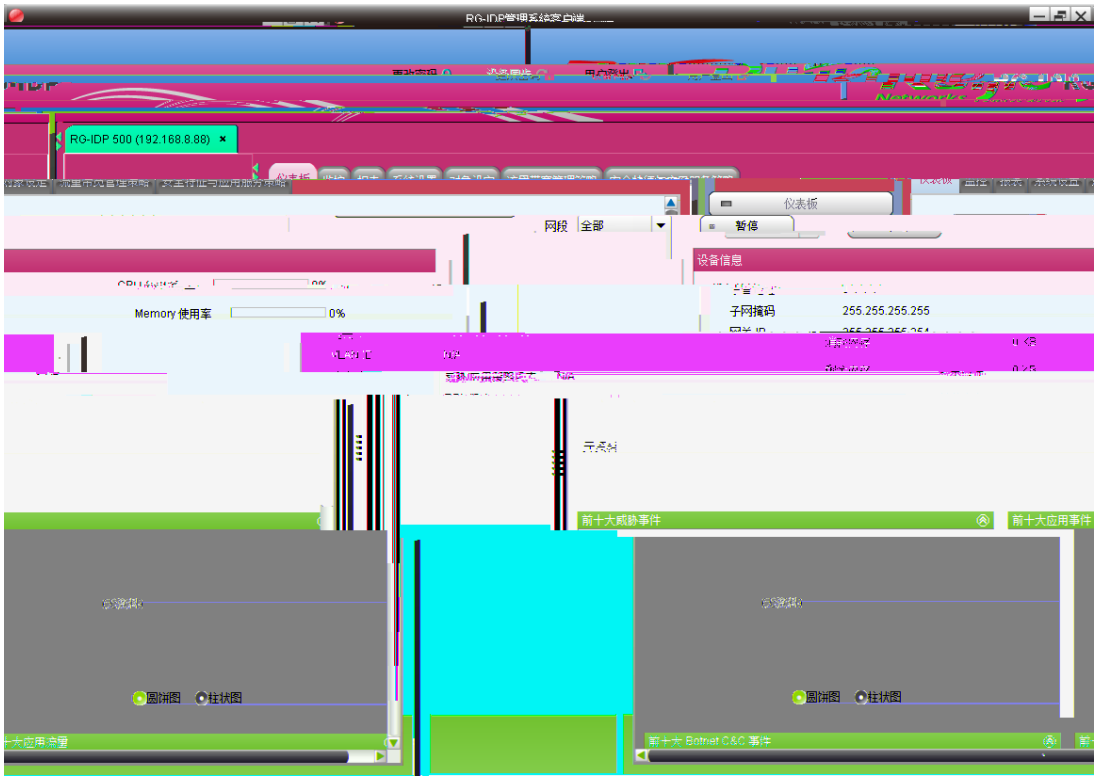
RG-IDP

2.2

2.4



2.5


RG-IDP 500 (192.168.8.88)
网段
全部
暂停
设备信息
Memory 使用率
0%
子网掩码
255.255.255.255
前十大威胁事件
前十大应用事件
圆饼图
柱状图

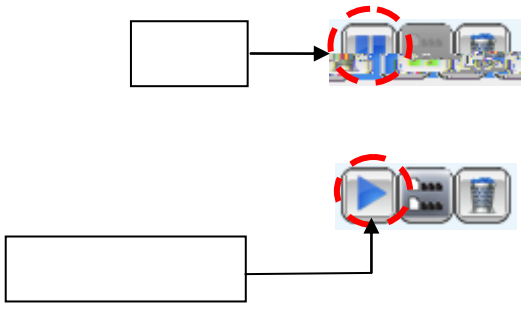
网段
全部
暂停
子网掩码
网关 IP
VLAN ID
N/A
RBL 版本
N/A

4

4.1

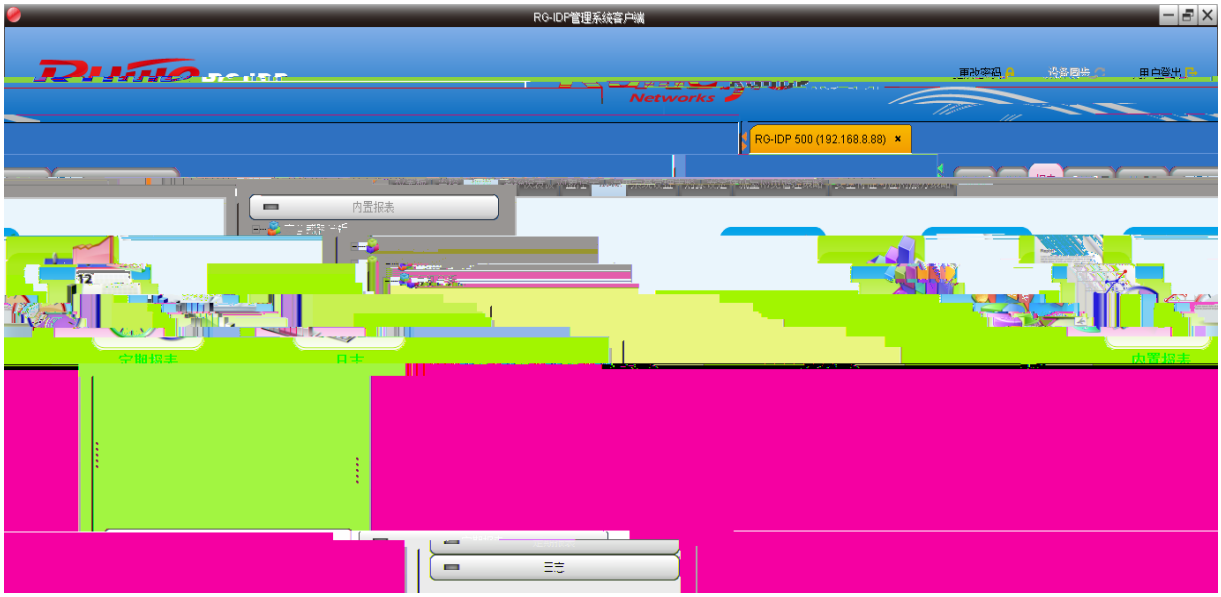
RG-IDP管理系统客户端
RG-IDP
RG-IDP 500 (192.168.8.88)
威胁
严重程度
网段
事件
预设反应
协议
索引
Extract REL

	列入流量限额黑名单 列入流量限额黑名单 流量限额使用率超过预警门坎



5

下



5.1 (Built-in Report)

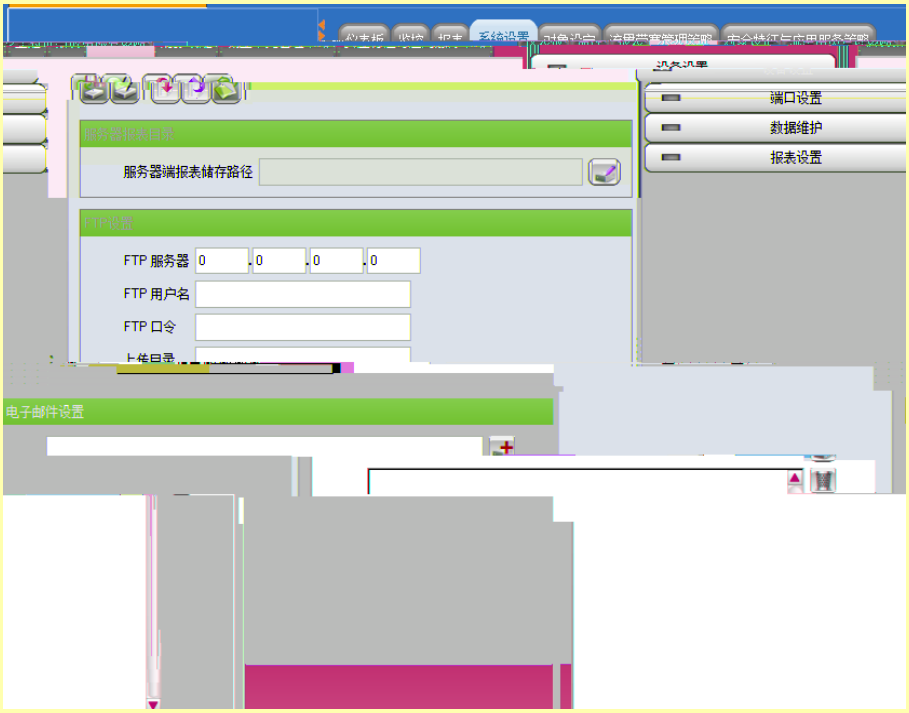
	两

5.1.1 (Threat Analysis)

5.1.2 Botnet (Botnet Analysis)

5.1.3 (Application Analysis)

	两

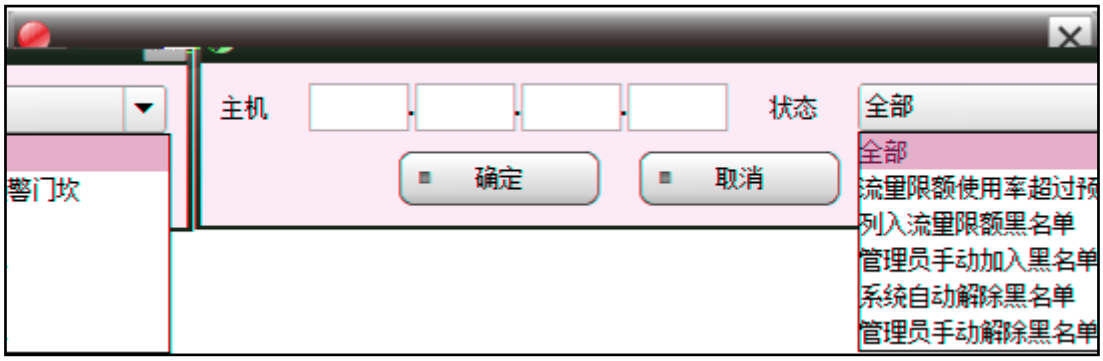


	不
	不
	不

5.3.2 Botnet C&C

5.3.6 (Blacklist)

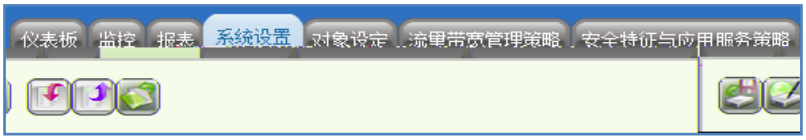
下

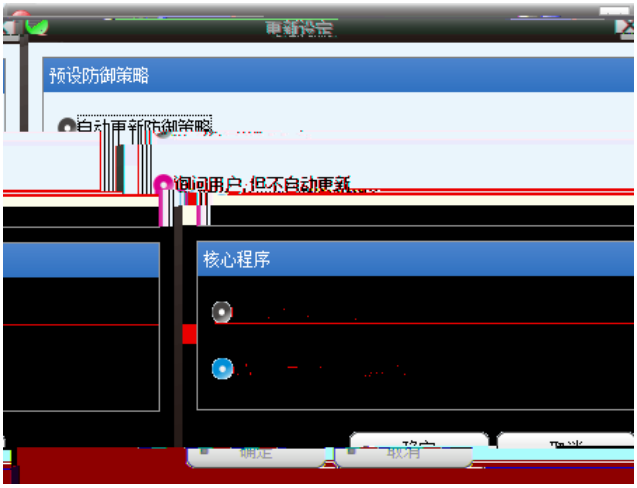


5.3.7 (System)

下

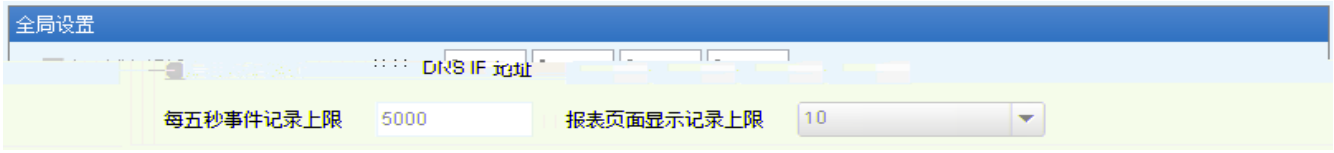
6



	两	
		

6.1 (Device Configuration)

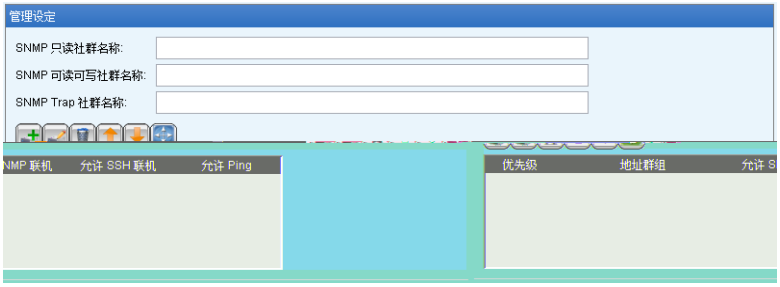
6.1.1



6.1.2 (Blacklist Configuration)

6.1.3 (Device Time Information)

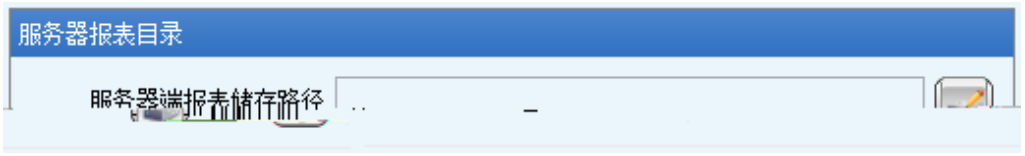
6.1.4 (Management Setting)



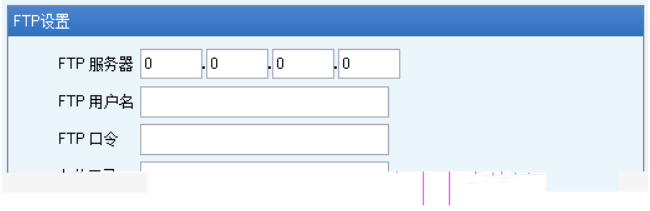
6.2

6.4

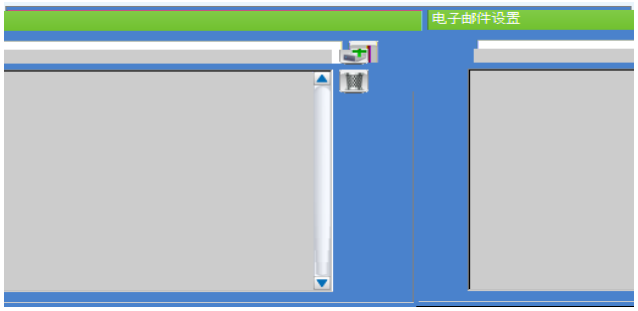
6.4.1



6.4.2 FTP



6.4.3



7

仪表板
监控
报表
系统设置
对象设定
流量带宽管理策略
安全特征与应用服务策略
地址群组
VLAN
时程
服务
目前IP对象数 0 / 最大IP对象数 1,023)
目前IP 群组数 0 / 最大IP 群组数 254)
IP 群组列表
编号
名称
IP对象数

7.1

	两	

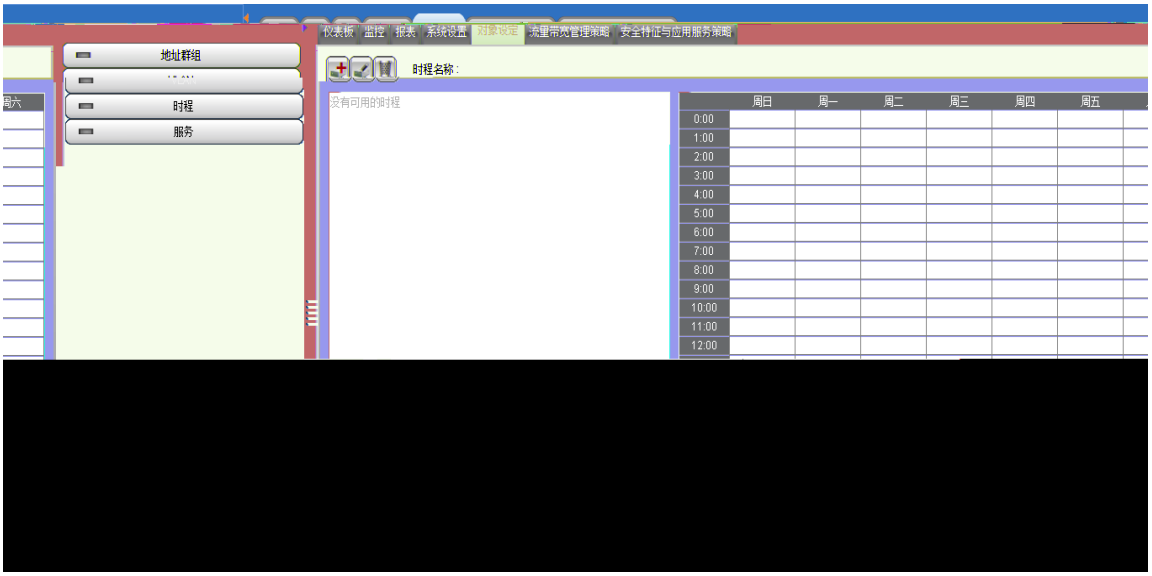
IP

7.2 VLAN

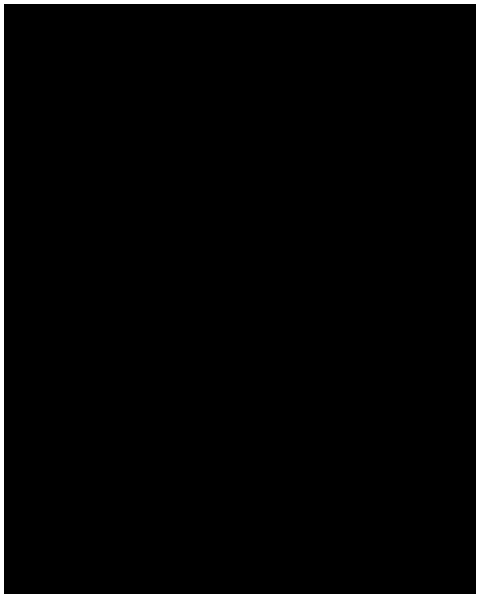
VLAN

修改 VLAN
VLAN 名称：
VLAN1
全选
全不选
编号
启用
VLAN ID
1
2
3
4
5
6
7
8
9
10
保存
取消

7.3

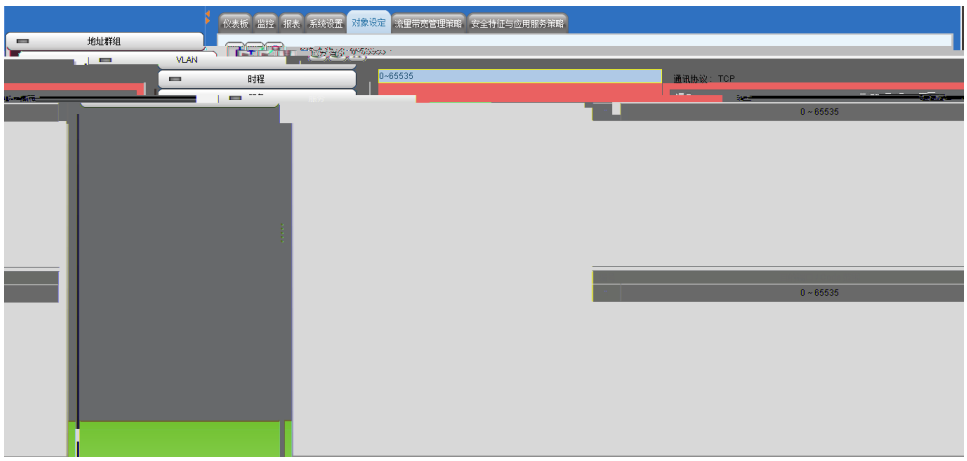

仪表板
监控
报表
系统设置
对象设定
流量带宽管理策略
安全特征与应用服务策略
地址群组
时程
服务
时程名称：
没有可用的时程
周日
周一
周二
周三
周四
周五
0:00
1:00
2:00
3:00
4:00
5:00
6:00
7:00
8:00
9:00
10:00
11:00
12:00

为



7.4

两



新增服务
服务名称：
通讯协议：
TCP
UDP
ICMP
0 ~ 65535
目的端口 / Code 范围
0 ~ 65535
保存
取消

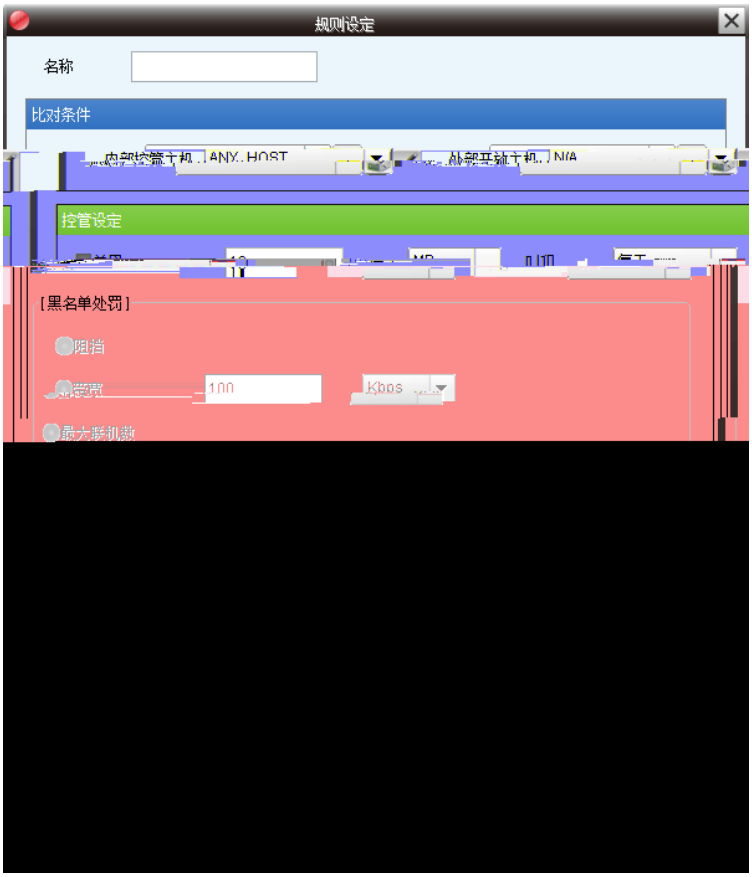
8

ÌÌ)ï° ^äYò1ËVñ B AÒ.€œ0P

8.2.1

8.2.2

	两	


规则设定
名称
比对条件
ANY, HOST
N/A
控管设定
[黑名单处罚]
阻挡
100
Kbps

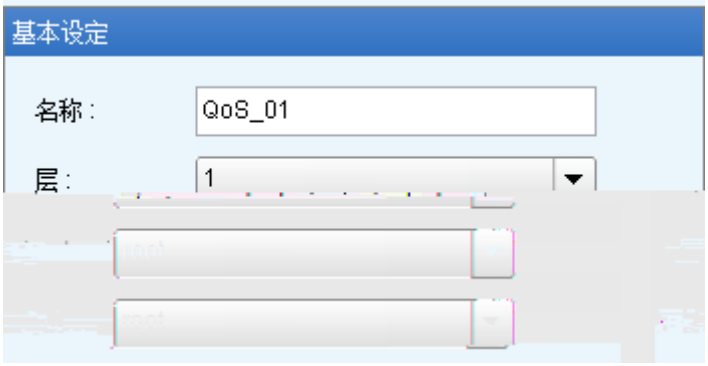
8.3.1

8.3.2

两

	两	

8.4.1



8.4.2

8.4.3

9

9.1.1

两

9.1.2

9.1.3 Botnet

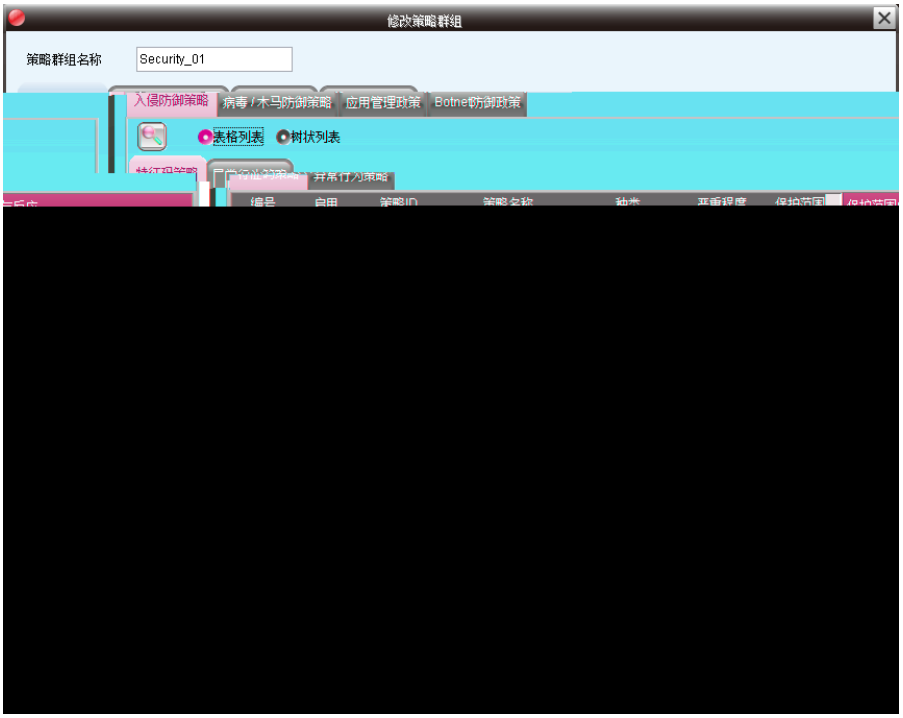
9.2

9.2.4

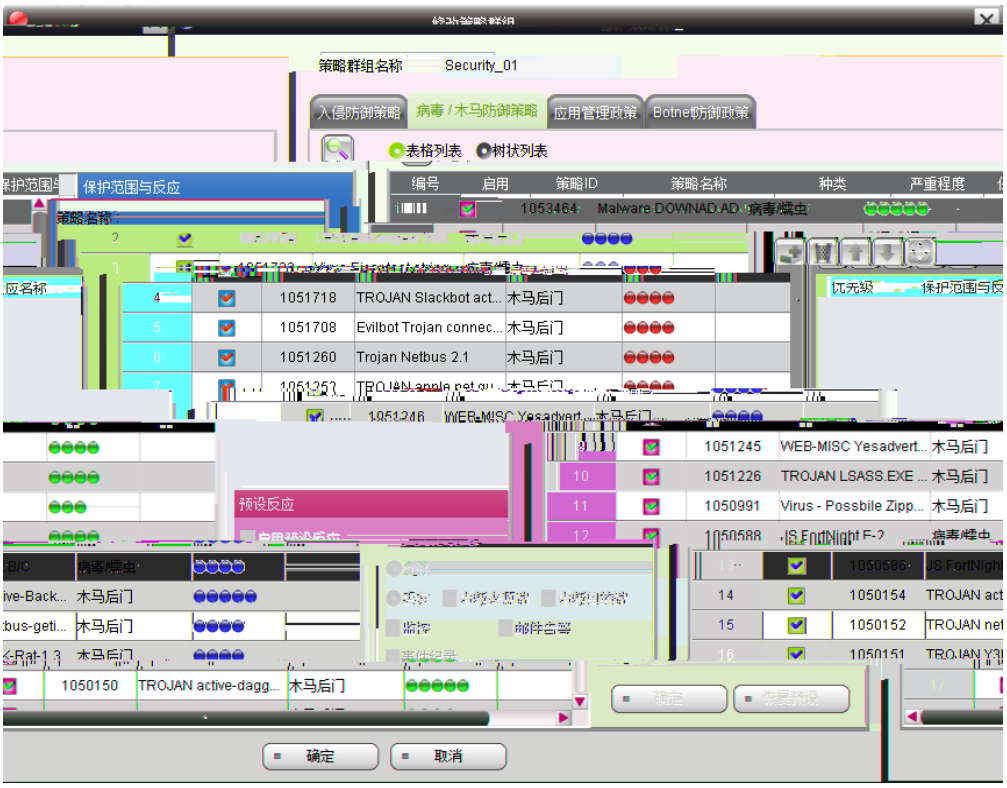
9.3

9.3.2

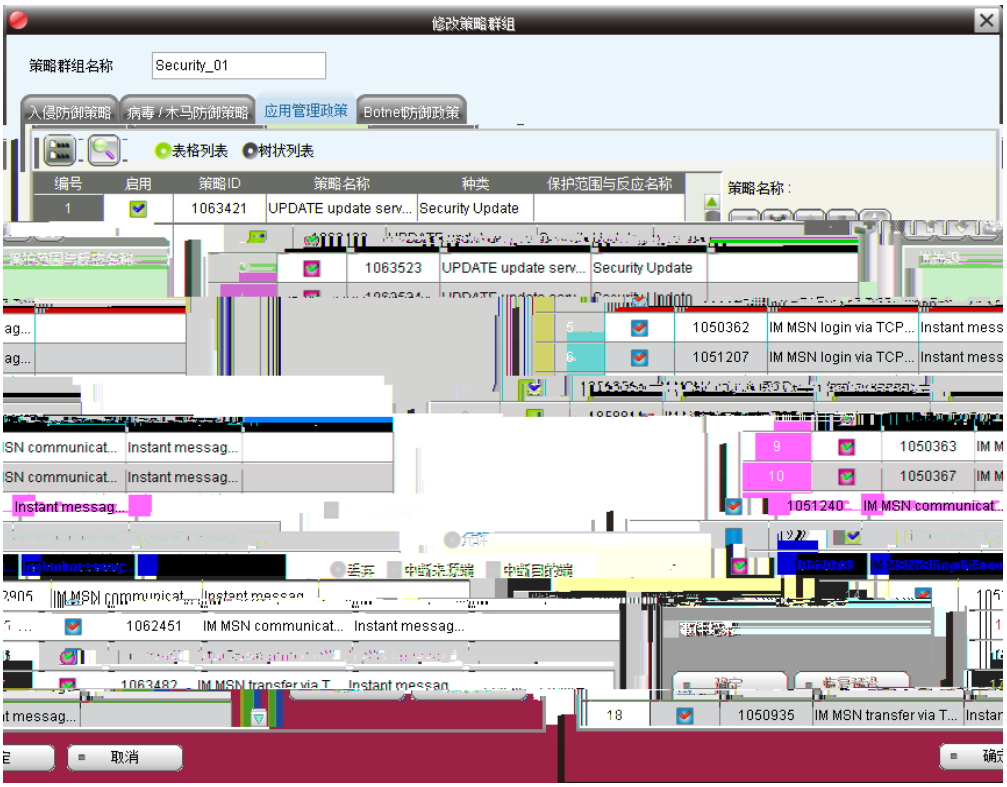
9.3.3


修改策略群组
策略群组名称
Security_01
入侵防御策略
病毒/木马防御策略
应用管理政策
Botnet防御政策
表格列表
树状列表

9.3.4

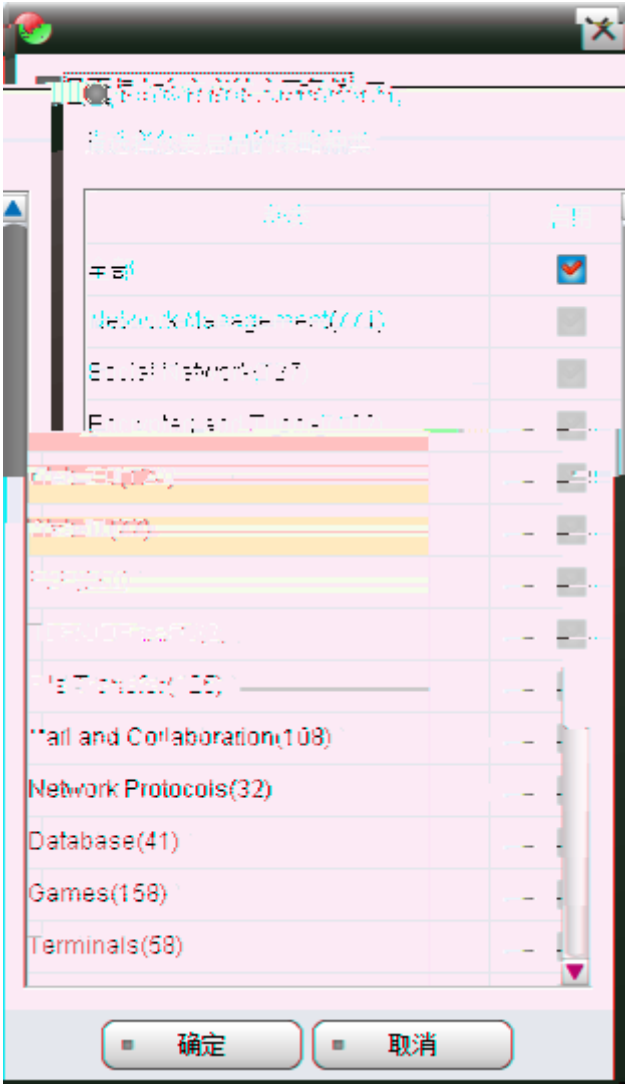

策略群组名称
Security_01
入侵防御策略
病毒/木马防御策略
应用管理政策
Botne防御政策
表格列表
树状列表
保护范围与反应
编号
启用
策略ID
策略名称
种类
严重程度
1053464
Malware.DOWNAD.AD
1051718
TROJAN Slackbot act...
木马后门
1051708
Evilbot Trojan connec...
1051260
Trojan Netbus 2.1
1051245
WEB-MISC Yesadvert...
1051226
TROJAN LSASS.EXE ...
1050991
Virus - Possbile Zipp...
预设反应
1050154
TROJAN act
1050152
TROJAN net
1050150
TROJAN active-dagg...
确定
取消

9.5


修改策略群组
策略群组名称
Security_01
入侵防御策略
病毒/木马防御策略
应用管理政策
Botnet防御政策
表格列表
树状列表
编号
启用
策略ID
策略名称
种类
保护范围与反应名称
策略名称：
1
1063421
UPDATE update serv...
Security Update
1063523
UPDATE update serv...
Security Update
1050362
IM MSN login via TCP...
1051207
IM MSN login via TCP...
1050363
1050367
1051240
IM MSN communicat...
1062451
IM MSN communicat...
Instant messag...
1063482
18
1050935
IM MSN transfer via T...
取消

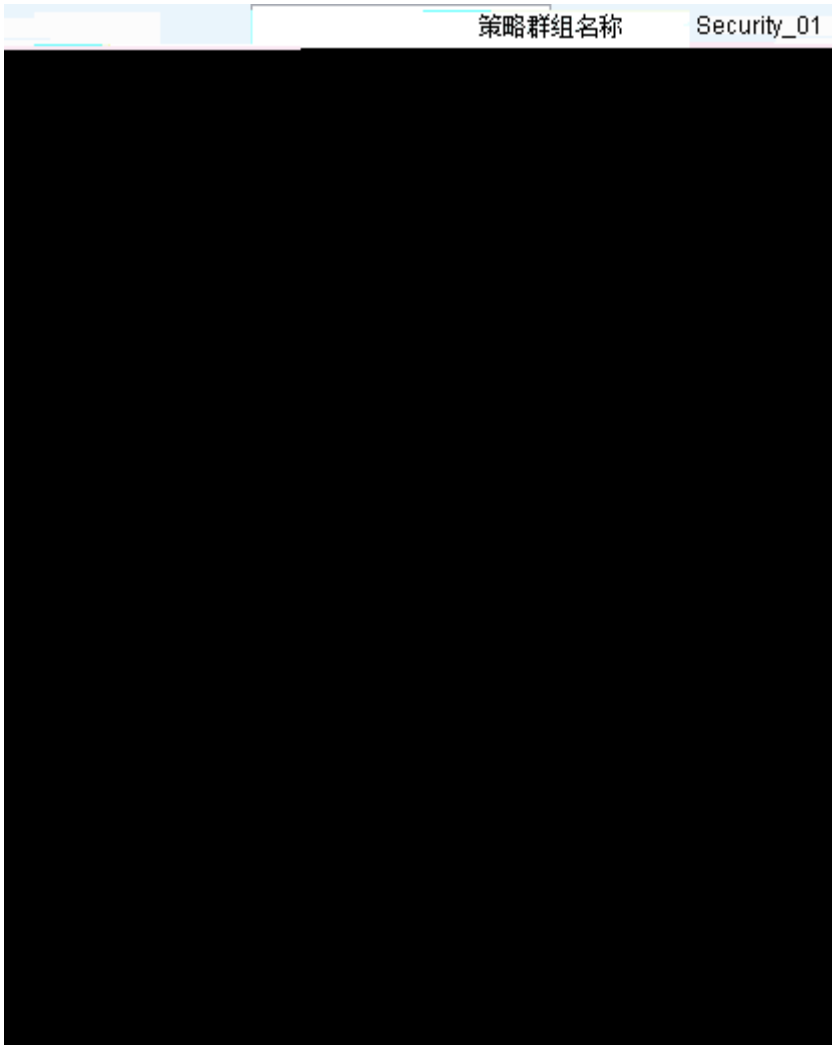
9.5.1

两

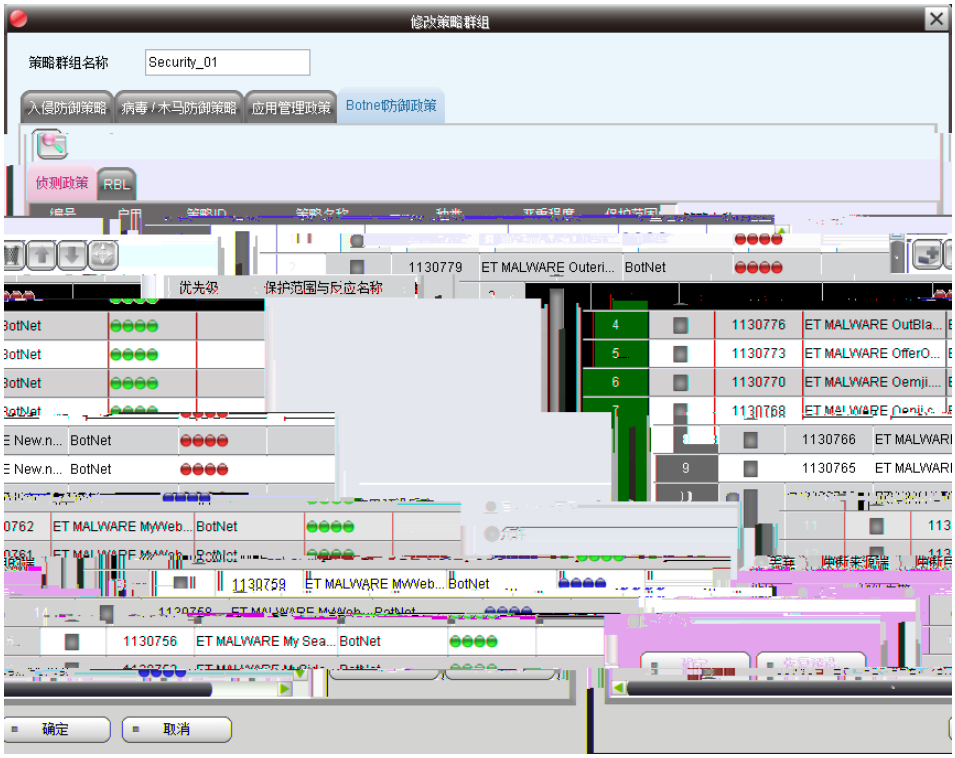

Network Protocols(32)
Database(41)
Games(158)
Terminals(58)
确定
取消

9.5.2

9.5.3

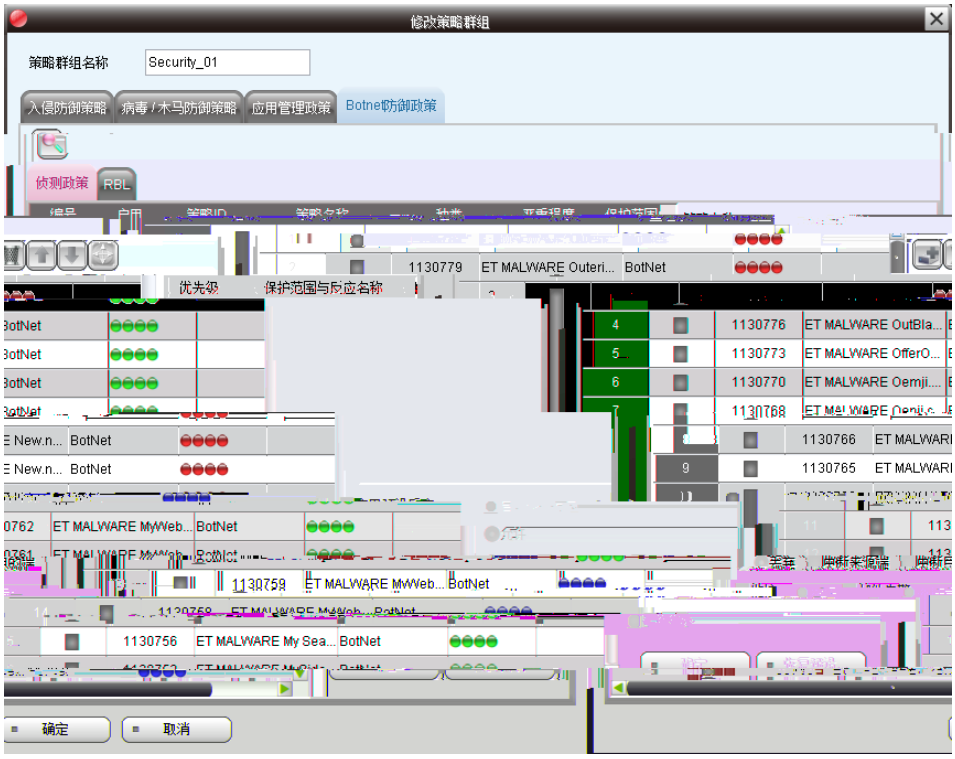


9.6 Botnet


修改策略群组
策略群组名称
Security_01
入侵防御策略
病毒/木马防御策略
应用管理政策
Botnet防御政策
侦测政策
RBL
优先级
保护范围与反应名称
1130779 ET MALWARE Outeri... BotNet
1130776 ET MALWARE OutBla...
1130773 ET MALWARE OfferO...
1130770 ET MALWARE Oemji...
1130766
1130765
1130759 ET MALWARE MyWeb... BotNet
1130756 ET MALWARE My Sea... BotNet
确定
取消

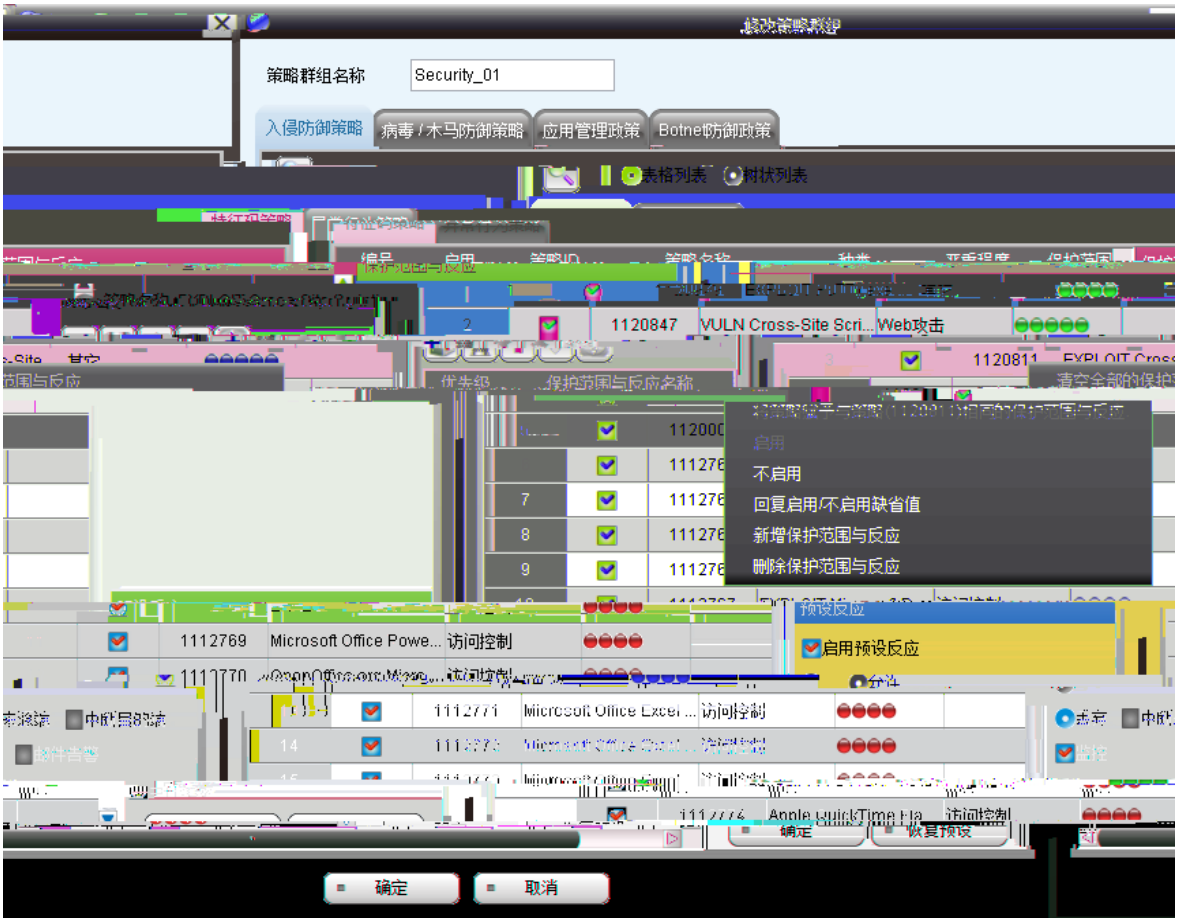
下

9.6.1


修改策略群组
策略群组名称
Security_01
入侵防御策略
病毒 / 木马防御策略
应用管理政策
Botnet防御政策
侦测政策
RBL
优先级
保护范围与反应名称
1130779 ET MALWARE Outeri... BotNet
1130776 ET MALWARE OutBla...
1130773 ET MALWARE OfferO...
1130770 ET MALWARE Oemji....
1130766
1130765
1130759 ET MALWARE MyWeb... BotNet
1130756 ET MALWARE My Sea... BotNet
确定
取消

9.6.2 RBL

9.7.1

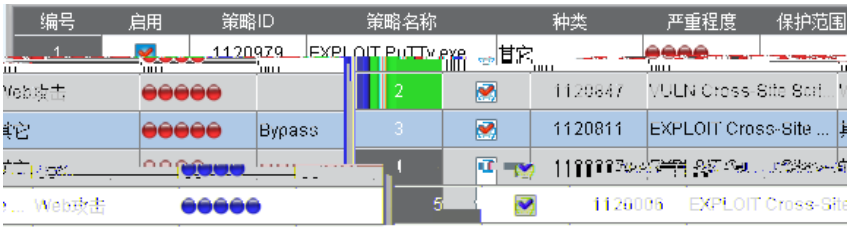

策略群组名称
Security_01
入侵防御策略
病毒/木马防御策略
应用管理政策
Botnet防御政策
表格列表
树状列表
1120847
VULN Cross-Site Scri...
Web攻击
不启用
回复启用/不启用缺省值
新增保护范围与反应
删除保护范围与反应
1112769
Microsoft Office Powe...
访问控制
启用预设反应
确定
取消

两

新增保护范围与反应
确定
取消

新增保护范围与反应
名称
保护范围
来源主机
1
目的主机
1
VLAN 群组
VLAN1
反应
允许
丢弃
中断来源端
中断目的端
监控
邮件告警
事件纪录
时程
确定

		两


编号
启用
策略ID
策略名称
种类
严重程度
保护范围
1120979
EXPLOIT PuTTy.exe
其它
Bypass
1120811
EXPLOIT Cross-Site ...
Web攻击
1120006

两 两

9.7.2

两 两

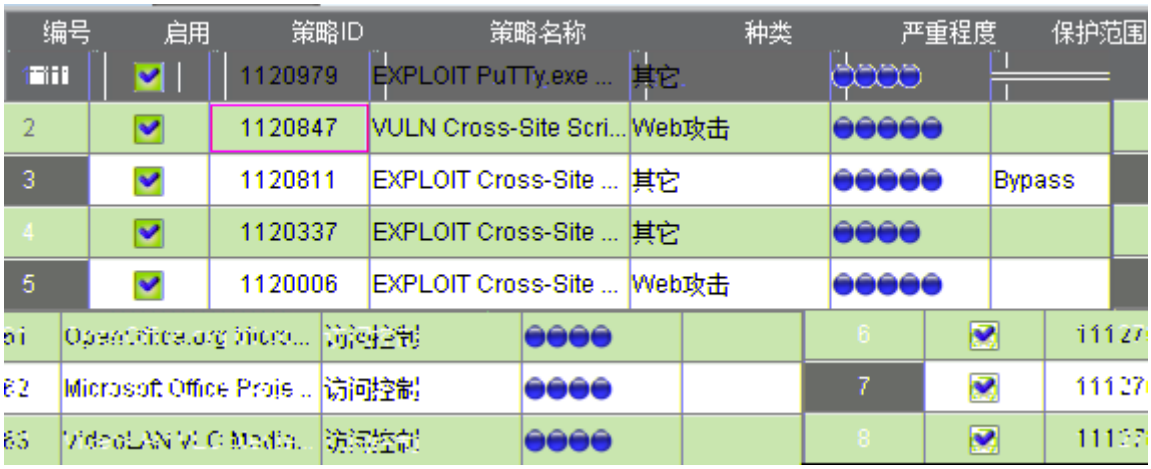
两 两

两

保护范围与反应
策略名称 :EXPLOIT Cross-Site Scripting ...
优先级
保护范围与反应名称
1
Bypass

9.8

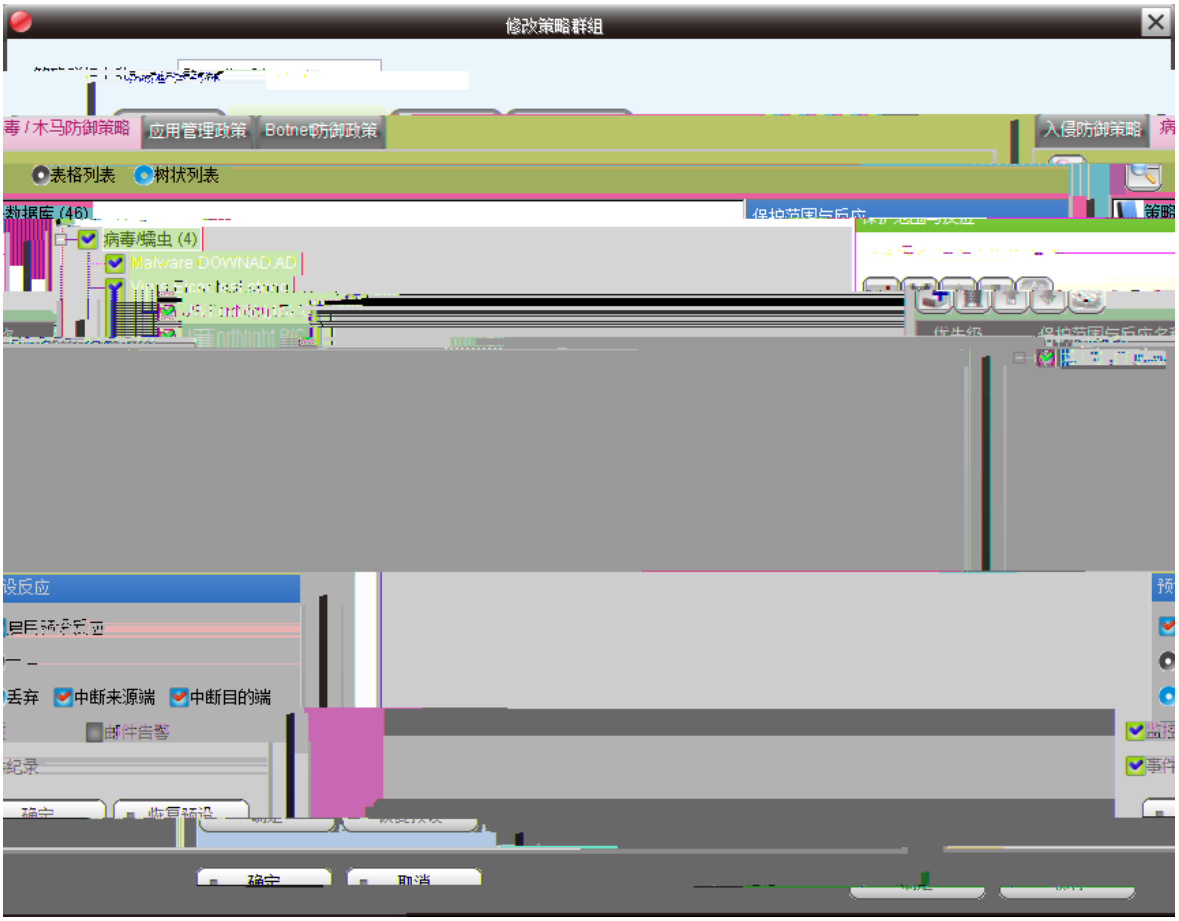
9.8.1 < >



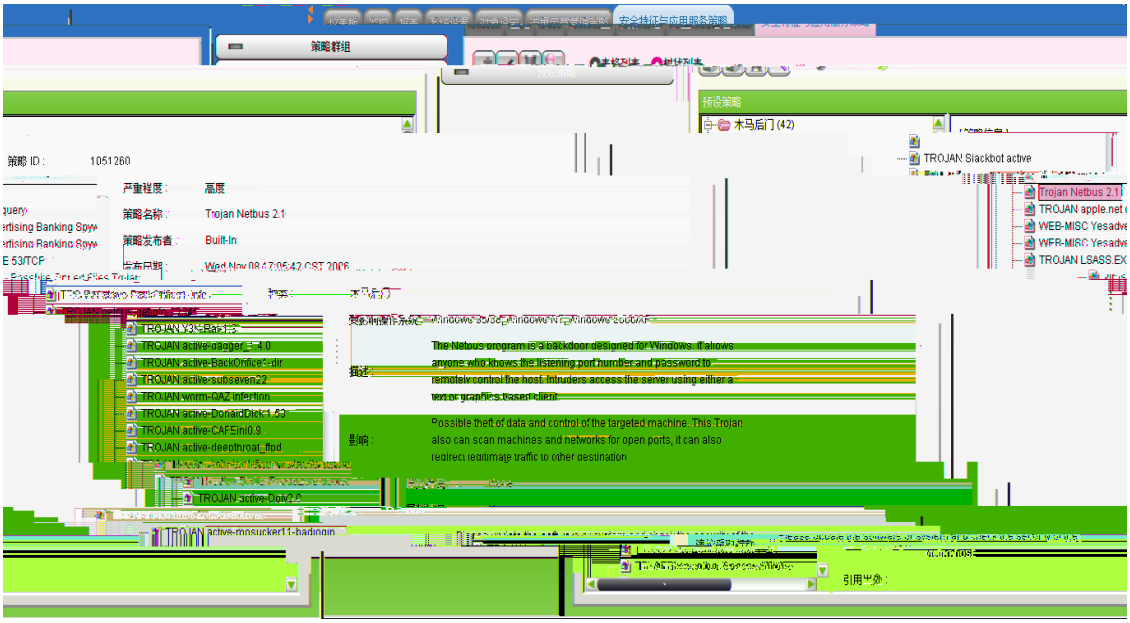
编号	启用	策略ID	策略名称	种类	严重程度	保护范围
	☑	1120979	EXPLOIT PuTTy.exe ...	其它	●●●●	
2	☑	1120847	VULN Cross-Site Scri...	Web攻击	●●●●●	
3	☑	1120811	EXPLOIT Cross-Site ...	其它	●●●●●	Bypass
4	☑	1120337	EXPLOIT Cross-Site ...	其它	●●●●	
5	☑	1120006	EXPLOIT Cross-Site ...	Web攻击	●●●●●	
81	OpenOffice.org Micro...	访问控制	●●●●		6	☑	111274
82	Microsoft Office Proje...	访问控制	●●●●		7	☑	111276
83	VideoLAN VLC Media...	访问控制	●●●●		8	☑	111277

9.8.2

9.8.4


修改策略群组
应用管理政策
Botnet防御政策
入侵防御策略
表格列表
树状列表
病毒/蠕虫 (4)
丢弃
中断来源端
中断目的端
确定
取消

9.8.5


策略群组
策略 ID：1051260
严重程度：高度
策略名称：Trojan Netbus 2.1
策略发布者：Built-In
TROJAN Blackbot active
Trojan Netbus 2.1
TROJAN active-mosucker11-badlogin
Please update the software or system and check the security of the
查找策略
分大小写
找下一个(F3)
找上一个(F4)