RG-IDP

V1.0

2.

3.

Enter a

a

1+ 2 Ctrl+Alt+A Ctrl

Alt A

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

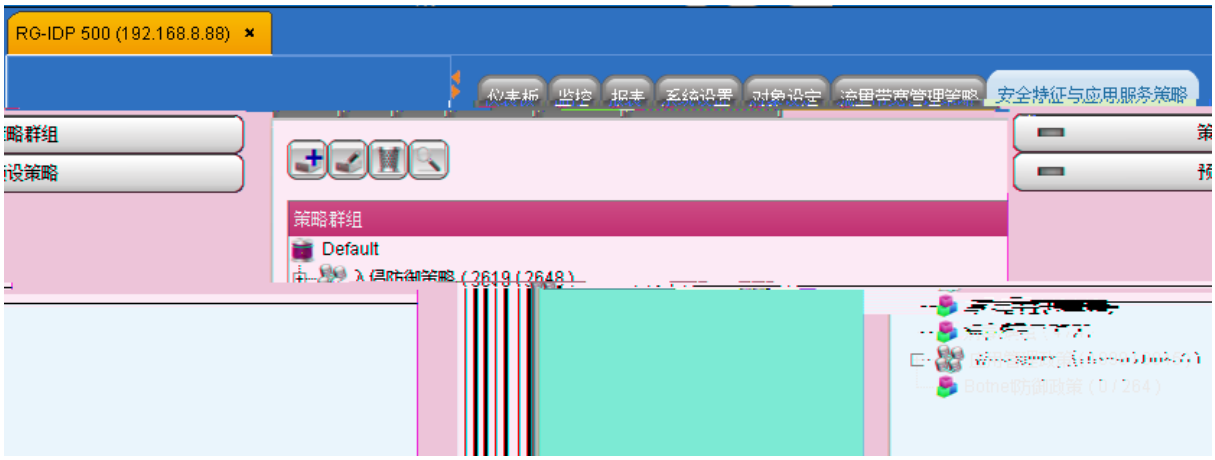
2

RG-IDP

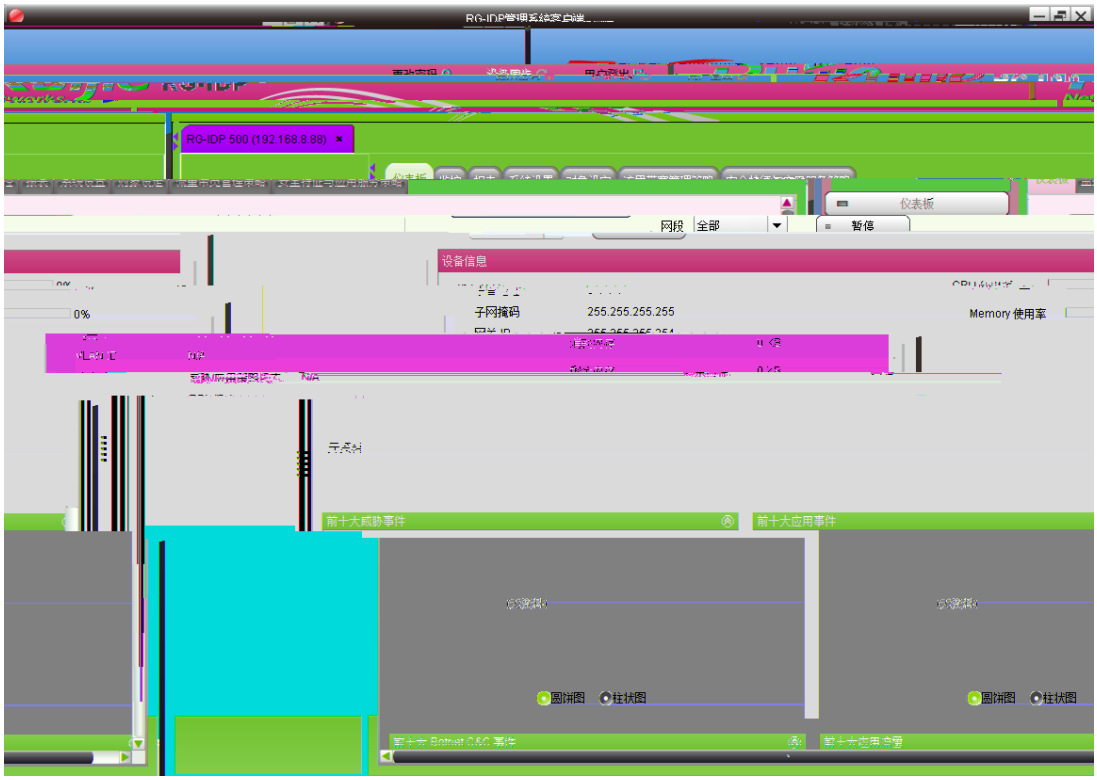
2.2

RG-IDP

2.4


RG-IDP 500 (192.168.8.88)
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
策略群组
Default

2.5

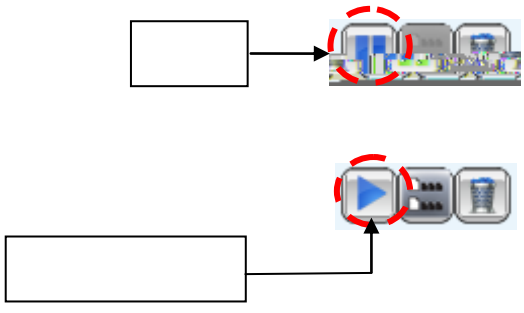

RG-IDP 500 (192.168.8.88)
仪表板
网段
全部
暂停
设备信息
子网掩码
255.255.255.255
Memory 使用率
前十大威胁事件
前十大应用事件
圆饼图
柱状图


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

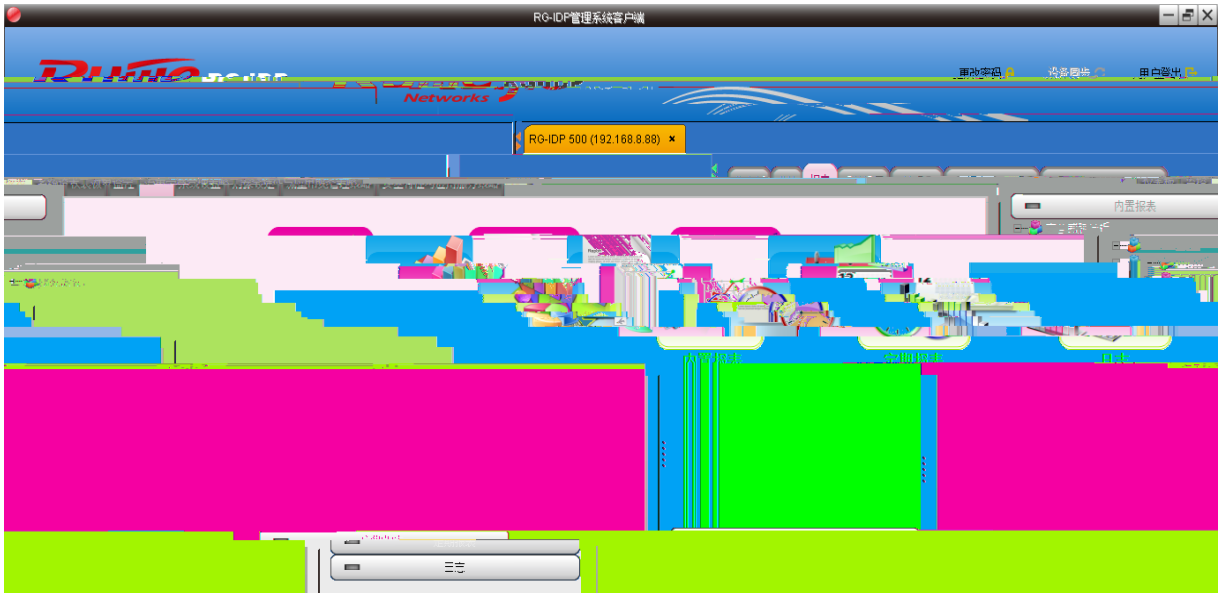
4

4.1

	 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



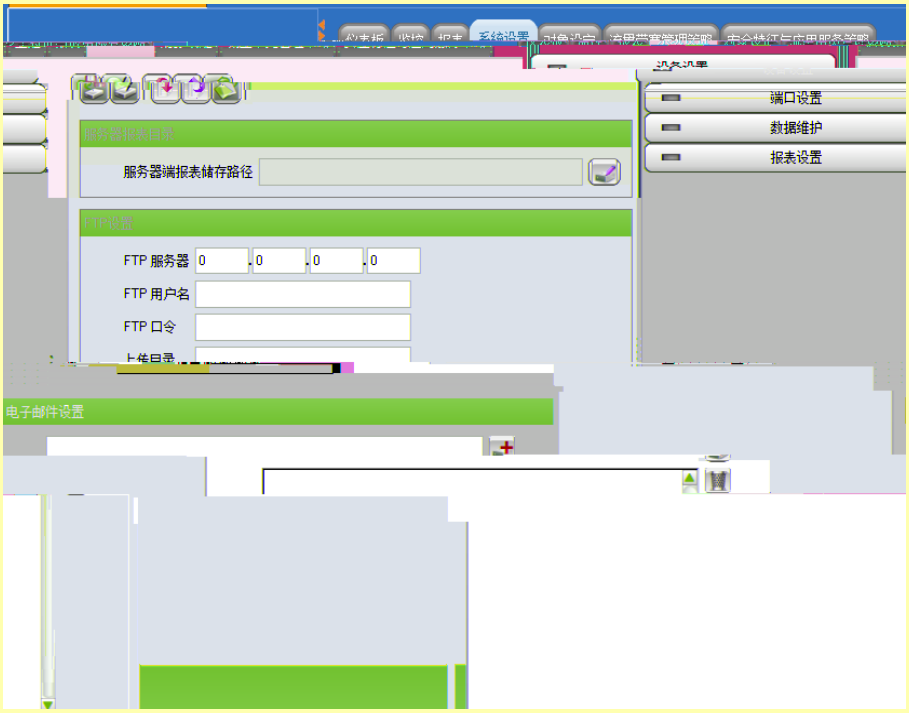
5.1 (Built-in Report)

5.1.1 (Threat Analysis)

5.1.2 Botnet (Botnet Analysis)

5.1.3 (Application Analysis)

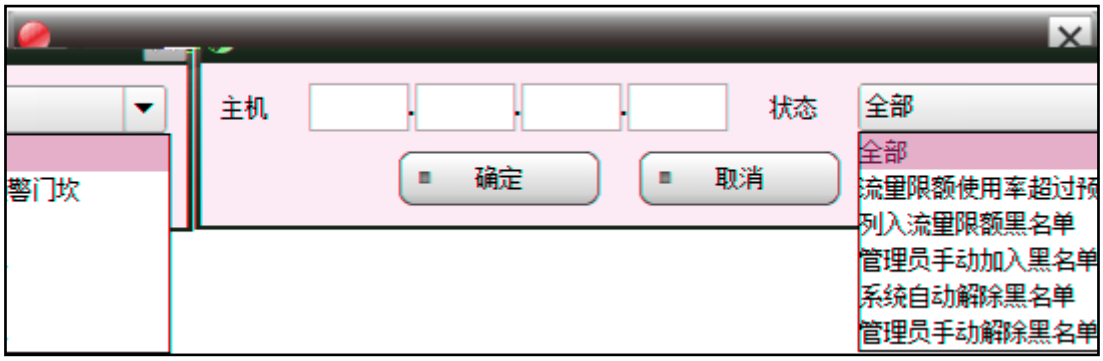
RG-IDP


端口设置
数据维护
报表设置
服务器端报表储存路径
FTP 服务器
FTP 用户名
FTP 口令
电子邮件设置

5.3.2 Botnet C&C

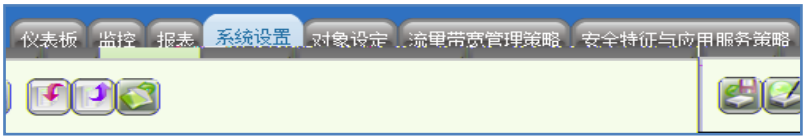
RG-IDP

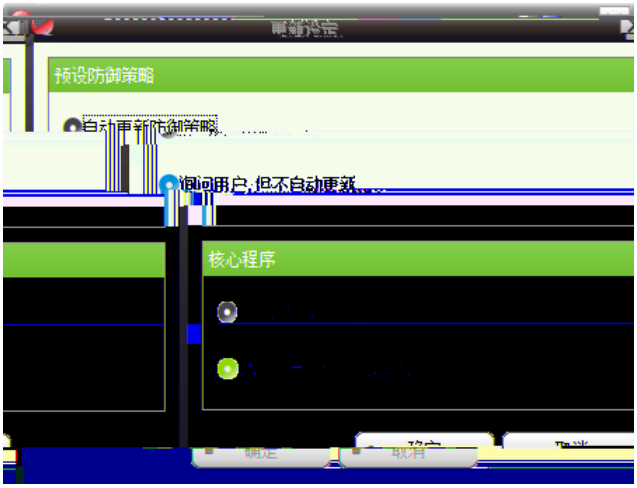
5.3.6 (Blacklist)



5.3.7 (System)

6

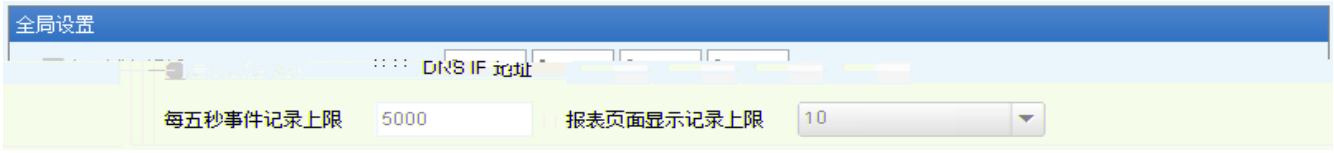


6.1 (Device Configuration)

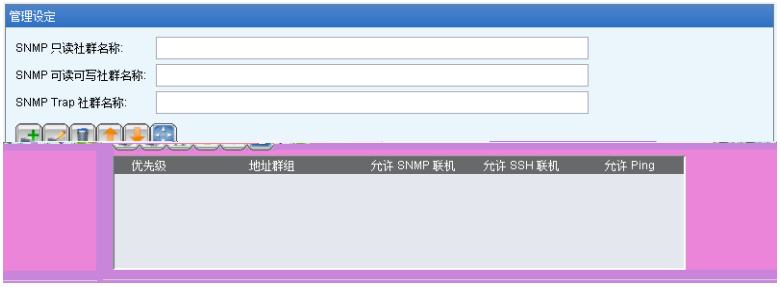
6.1.1



6.1.2 (Blacklist Configuration)

6.1.3 (Device Time Information)

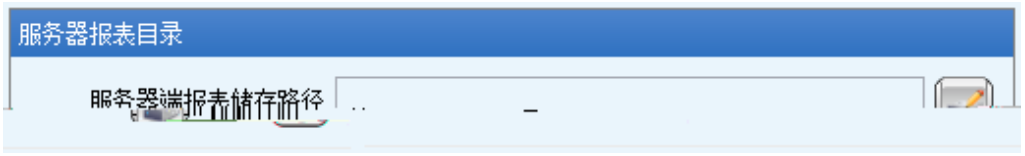
6.1.4 (Management Setting)



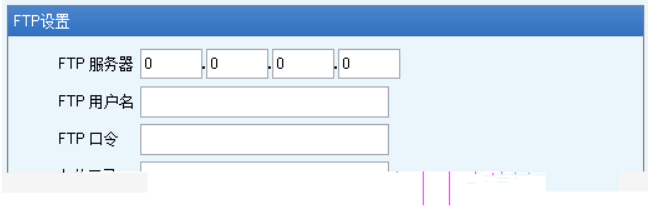
6.2

6.4

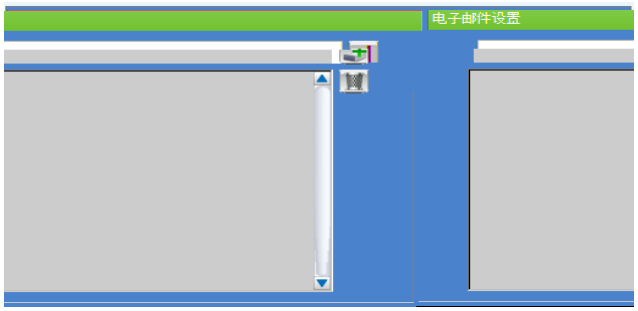
6.4.1



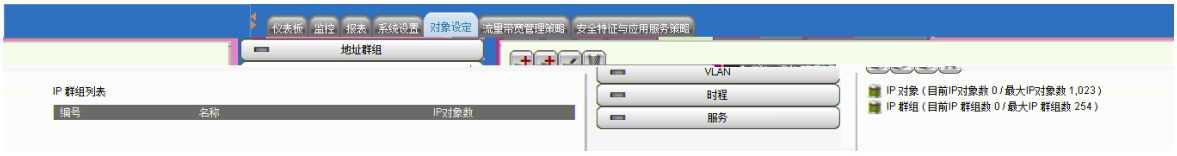
6.4.2 FTP



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
IP 群组列表
编号
名称
IP对象数
IP 对象（目前IP对象数 0 / 最大IP对象数 1,023）
IP 群组（目前IP 群组数 0 / 最大IP 群组数 254）

7.1

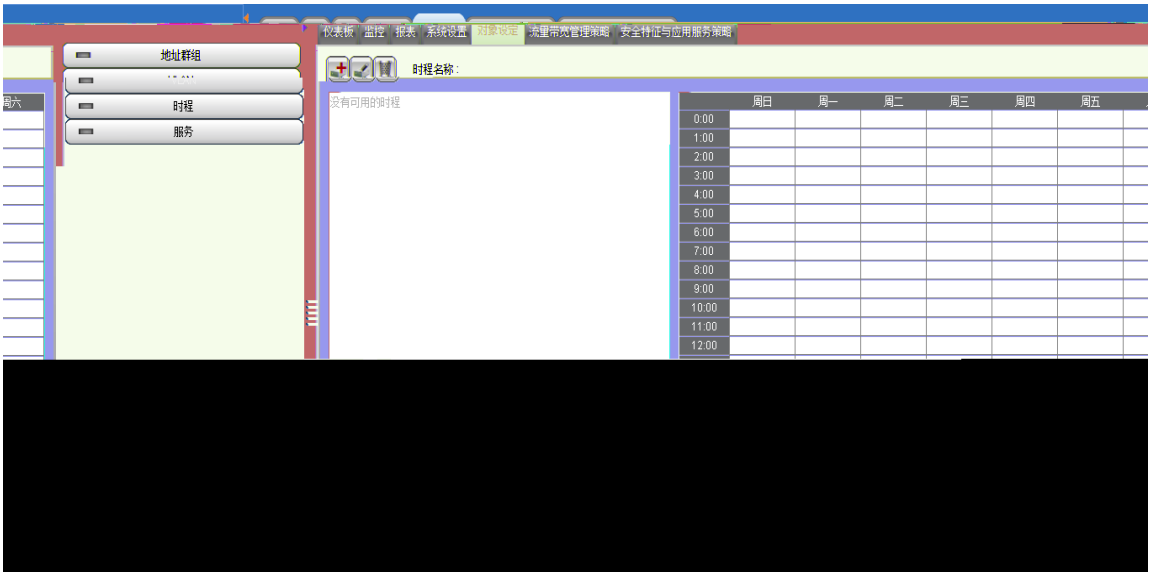
IP

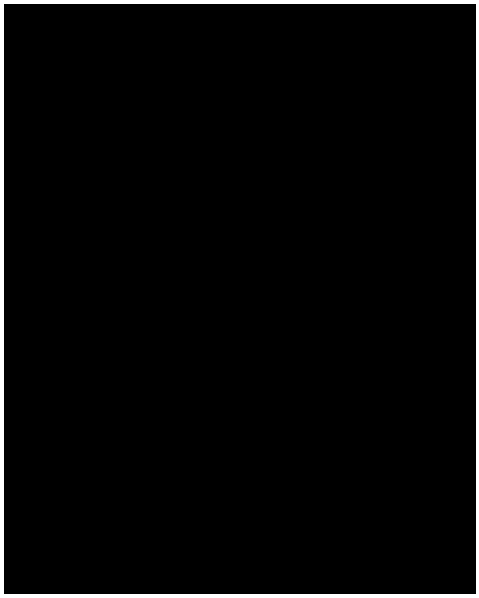
7.2 VLAN

VLAN

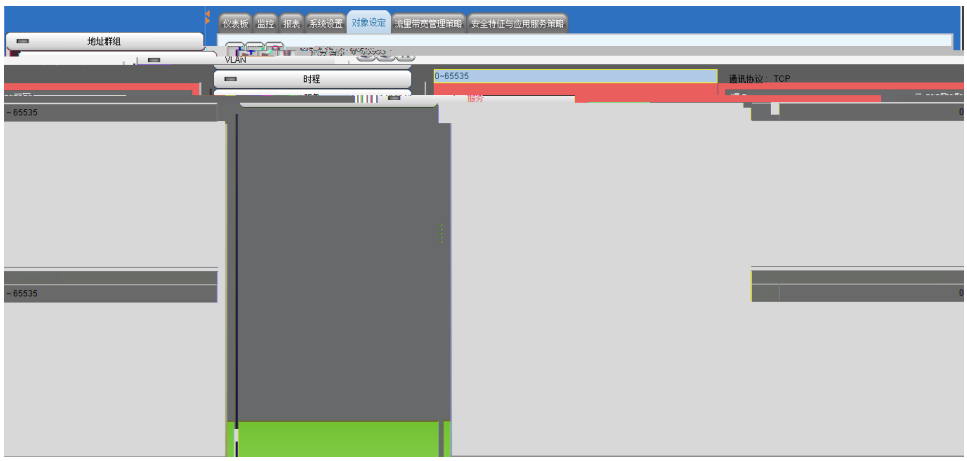

修改 VLAN
VLAN 名称：
VLAN1
全选
全不选
编号
启用
VLAN ID
1
2
3
4
5
6
7
8
9
10
保存
取消

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



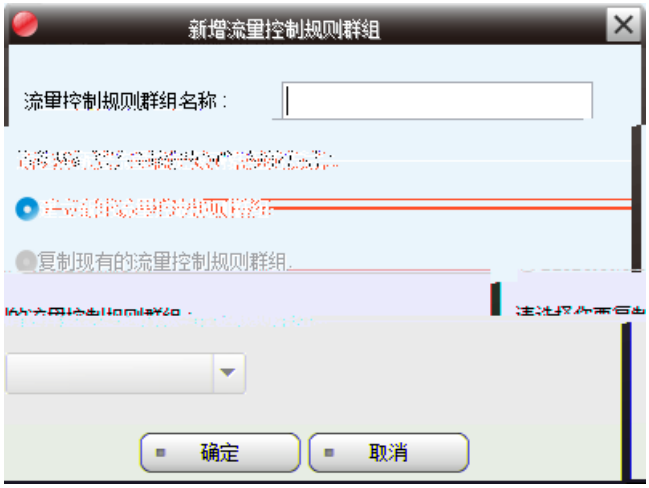
7.4




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

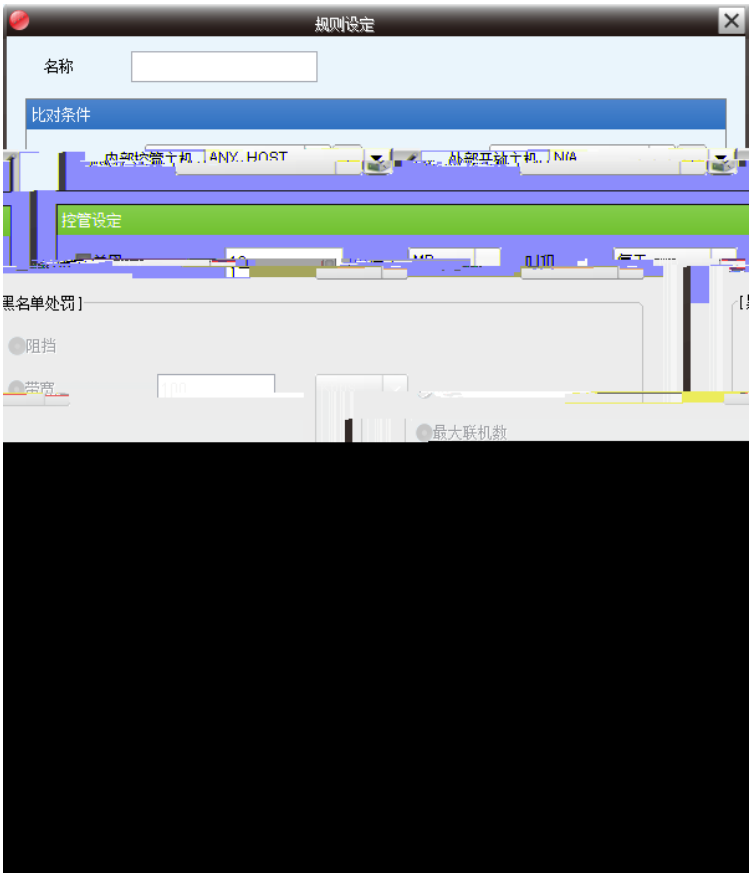
8.2.1



8.2.2


名称：
QOs_01
上行之总带宽
1,000,000
Kbps
名称
状态
内部控管主机
外部开放主机
时程
带宽
总量

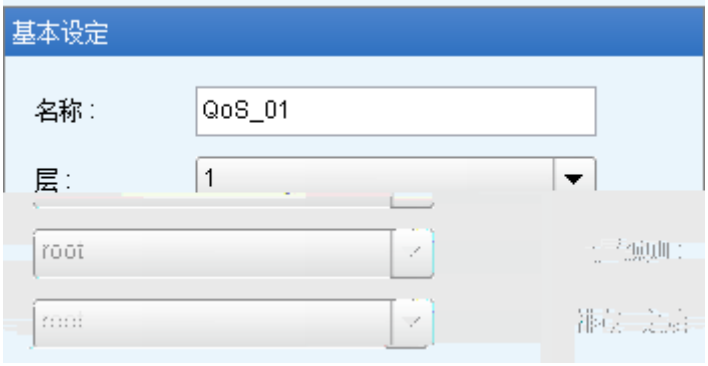

规则设定
名称
比对条件
ANY, HOST
N/A
控管设定
阻挡
最大联机数

8.3.1

8.3.2

8.4.1



8.4.2

8.4.3

9

9.1.1

9.1.2

9.1.3 Botnet

9.2

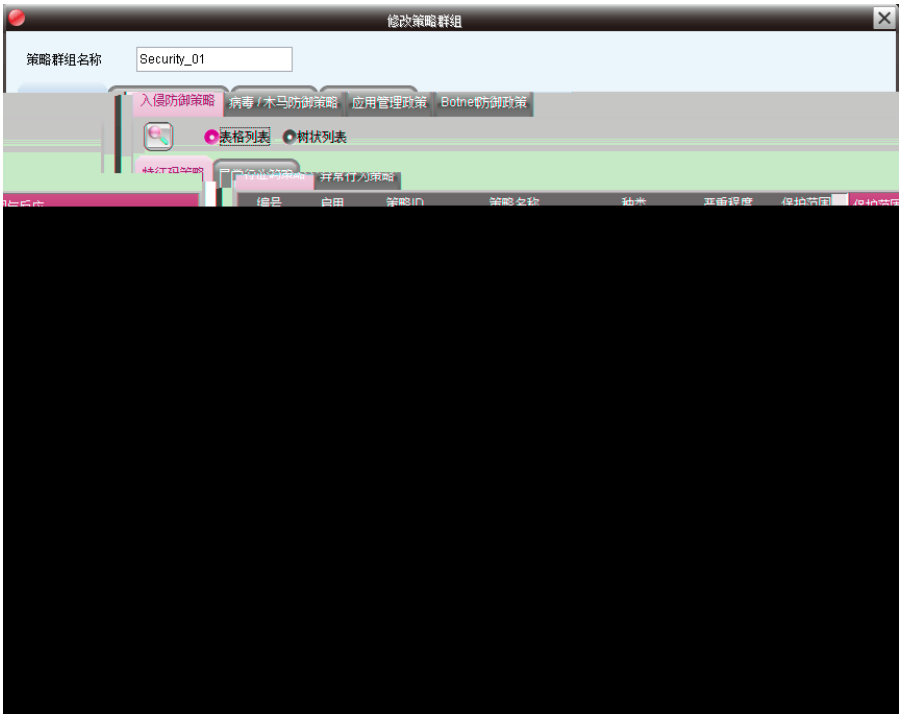
RG-IDP

9.2.4

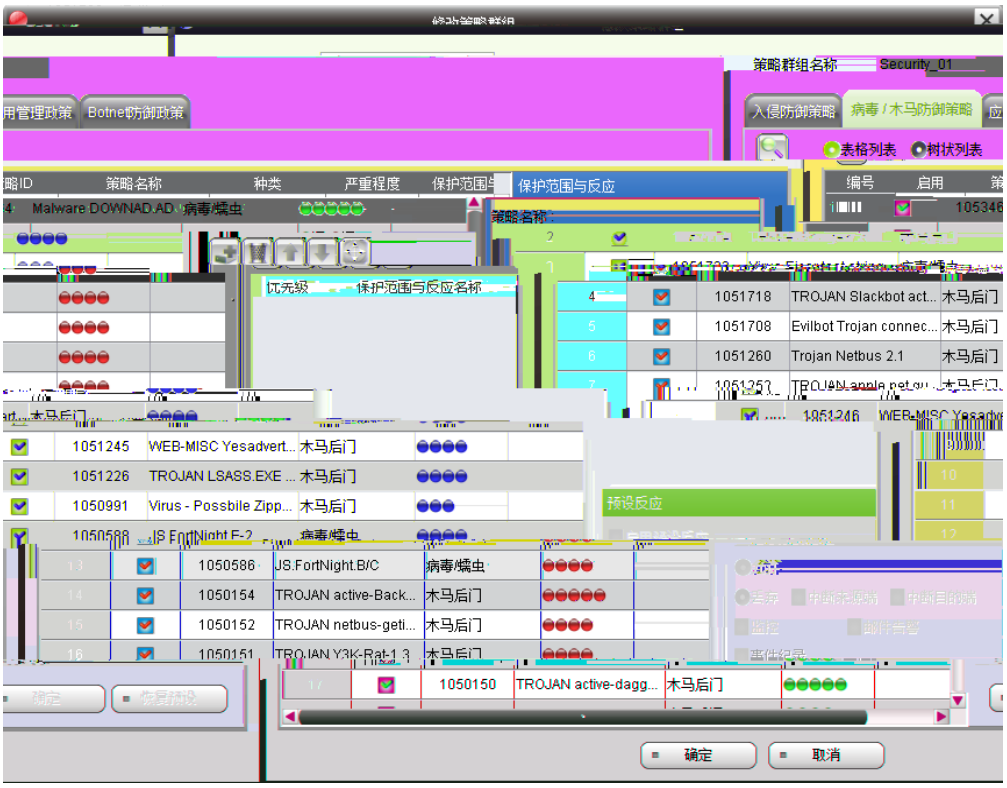
9.3

9.3.2

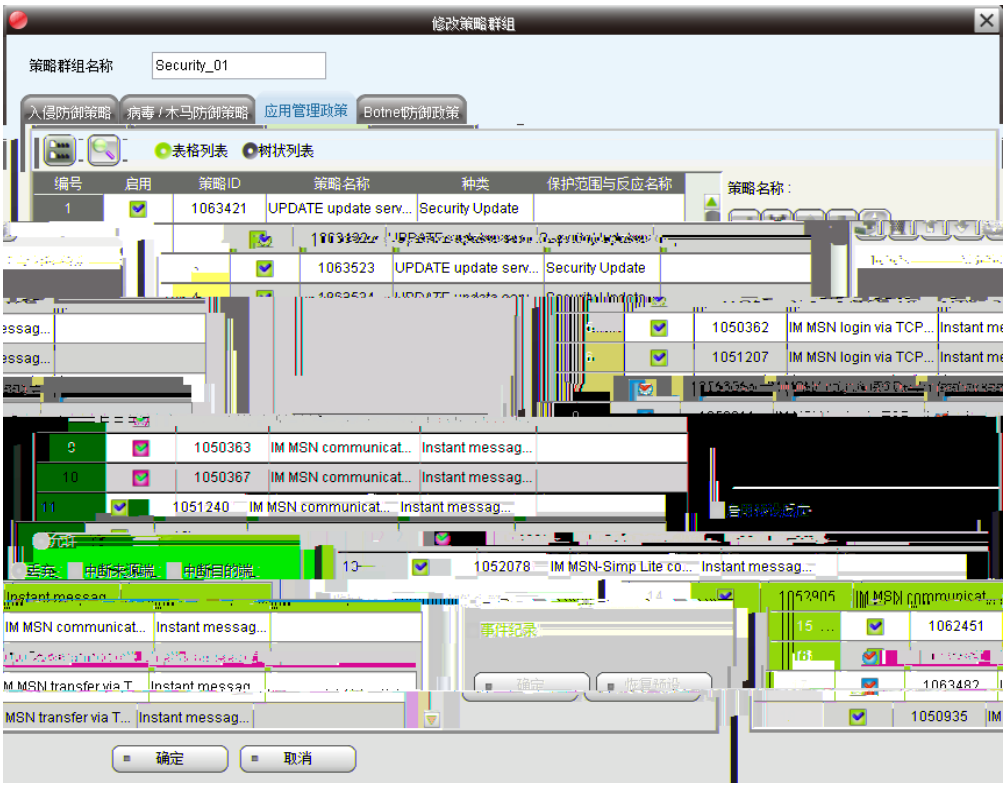
9.3.3


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

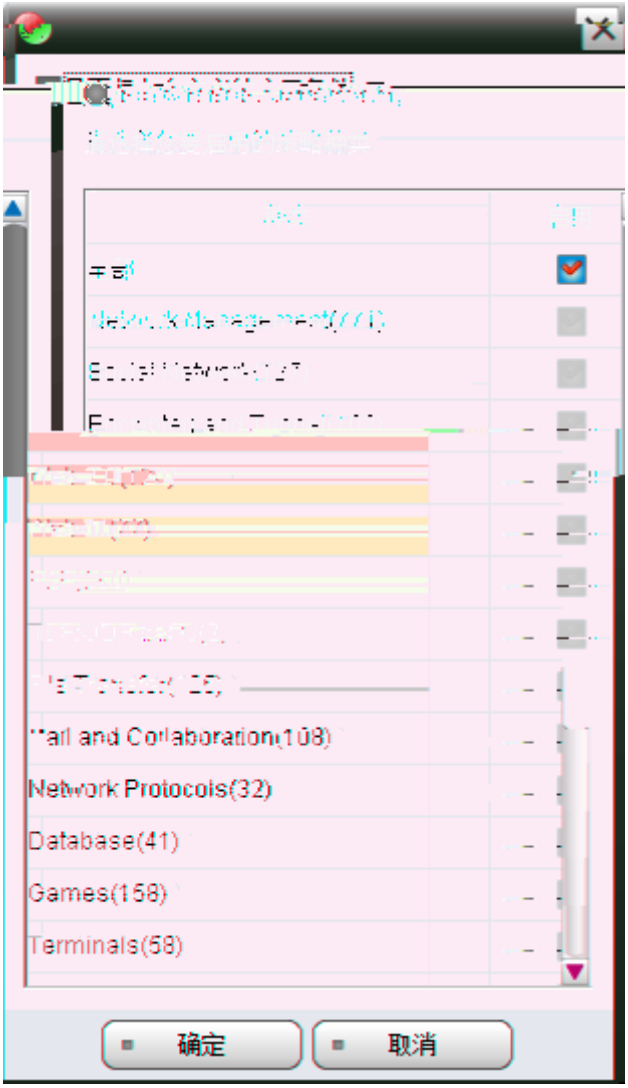
9.3.4


策略群组名称
Security_01
入侵防御策略
病毒/木马防御策略
表格列表
树状列表
策略ID
策略名称
种类
严重程度
保护范围与反应
编号
启用
1051718 TROJAN Slackbot act... 木马后门
1051708 Evilbot Trojan connec... 木马后门
1051260 Trojan Netbus 2.1 木马后门
1051245 WEB-MISC Yesadvert... 木马后门
1051226 TROJAN LSASS.EXE ... 木马后门
1050991 Virus - Possbile Zipp... 木马后门
1050586 JS.FortNight.B/C 病毒蠕虫
1050154 TROJAN active-Back... 木马后门
1050152 TROJAN netbus-geti... 木马后门
1050150 TROJAN active-dagg... 木马后门
预设反应
确定
取消

9.5

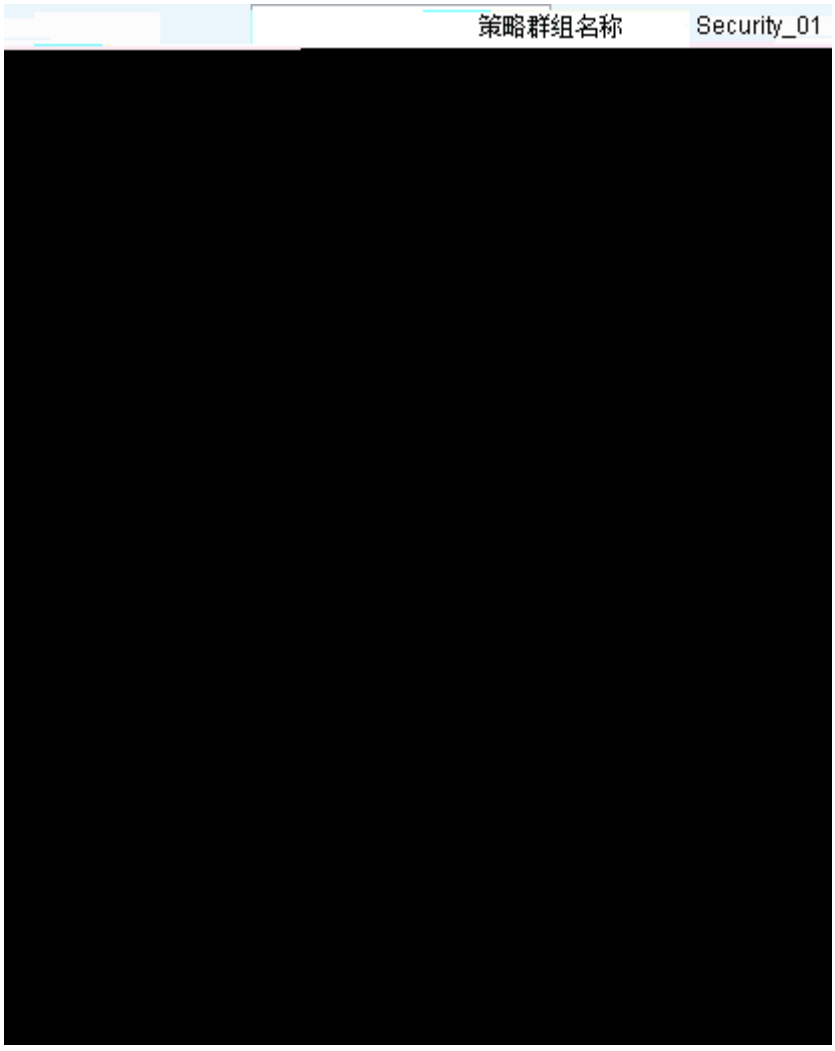

修改策略群组
策略群组名称
Security_01
入侵防御策略
病毒/木马防御策略
应用管理政策
Botnet防御政策
表格列表
树状列表
编号
启用
策略ID
策略名称
种类
保护范围与反应名称
策略名称：
1
1063421
UPDATE update serv...
Security Update
1063523
UPDATE update serv...
Security Update
1050362
IM MSN login via TCP...
1051207
IM MSN login via TCP...
1050363
IM MSN communicat...
Instant messag...
1050367
IM MSN communicat...
Instant messag...
1051240
IM MSN communicat...
Instant messag...
1052078
IM MSN-Simp Lite co...
Instant messag...
事件纪录
1062451
1050935
确定
取消

9.5.1

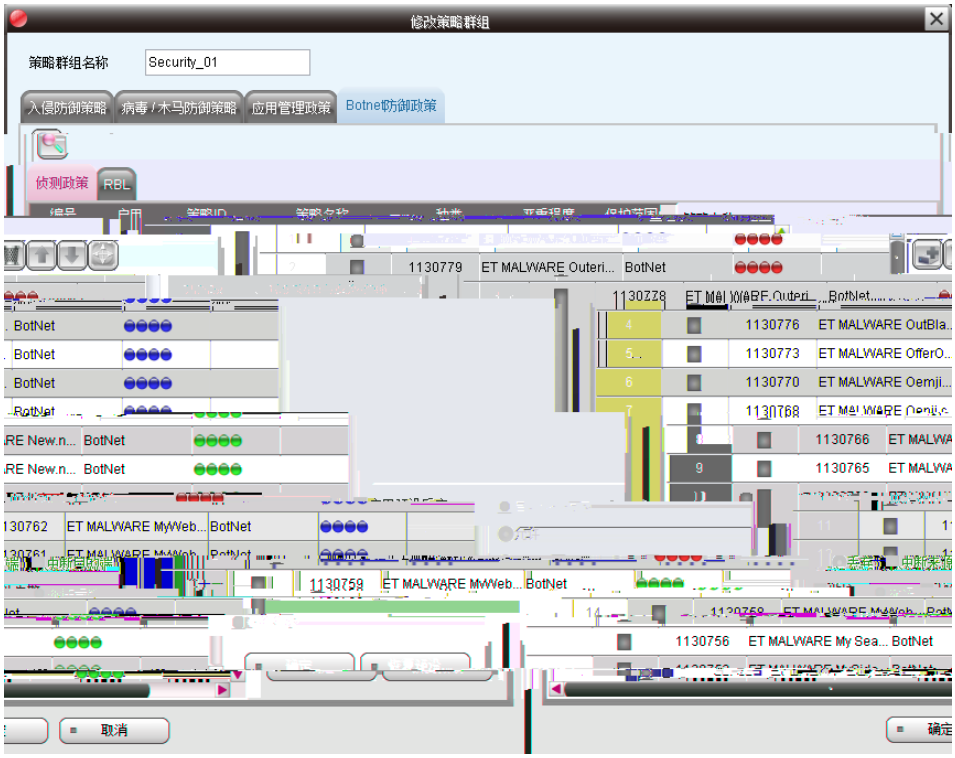

Network Protocols(32)
Database(41)
Games(158)
Terminals(58)
确定
取消

9.5.2

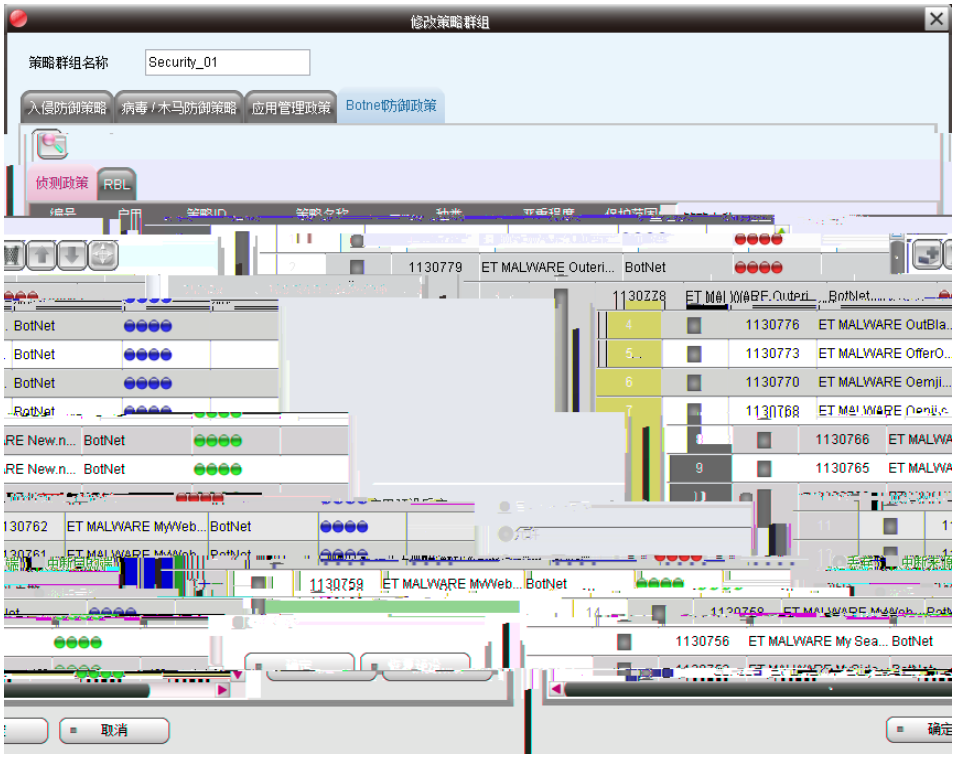
9.5.3



9.6 Botnet

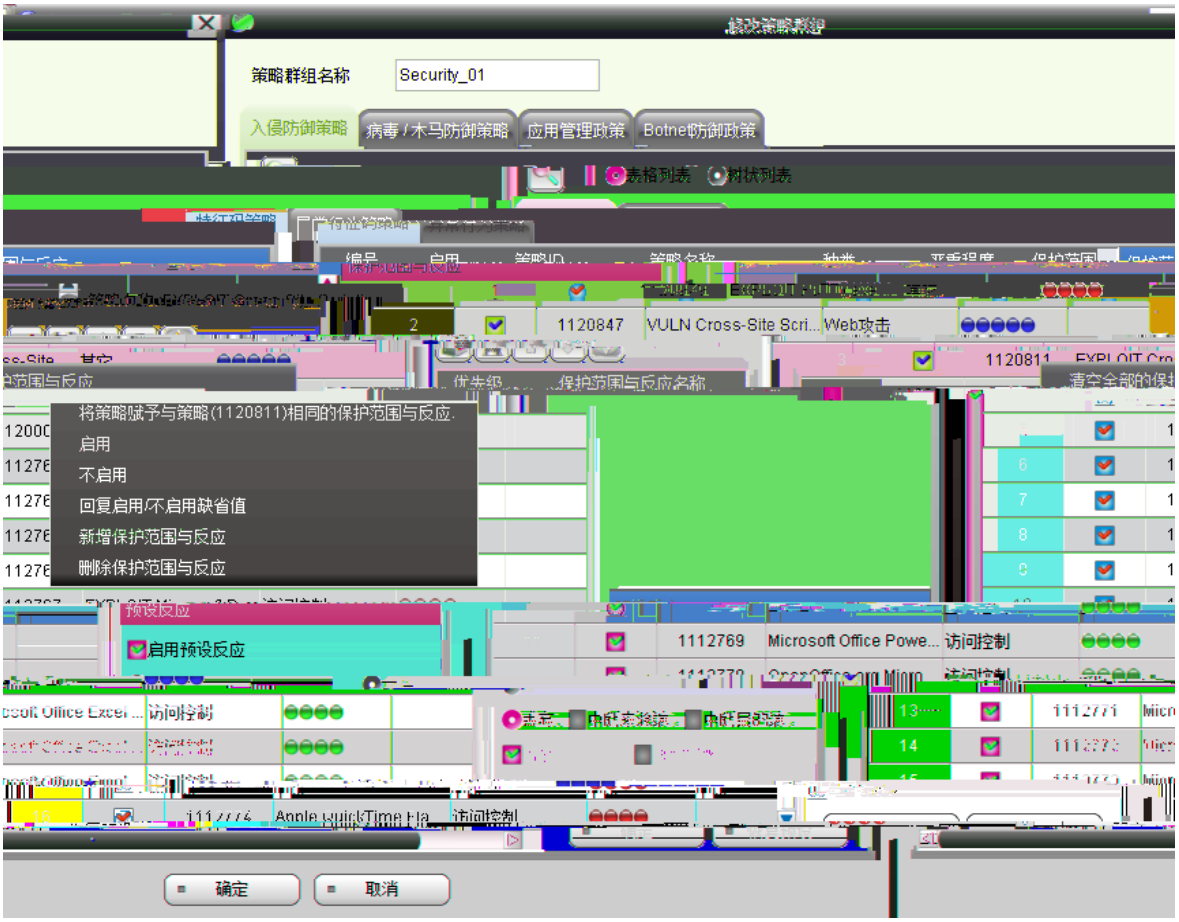

修改策略群组
策略群组名称
Security_01
入侵防御策略
病毒/木马防御策略
应用管理政策
Botnet防御政策
侦测政策
RBL
1130779 ET MALWARE Outeri... BotNet
BotNet
BotNet
BotNet
1130776 ET MALWARE OutBla...
1130773 ET MALWARE OfferO...
1130770 ET MALWARE Oemji...
1130766
1130765
1130762 ET MALWARE MyWeb... BotNet
1130759 ET MALWARE MyWeb... BotNet
1130756 ET MALWARE My Sea... BotNet
取消
确定

9.6.1

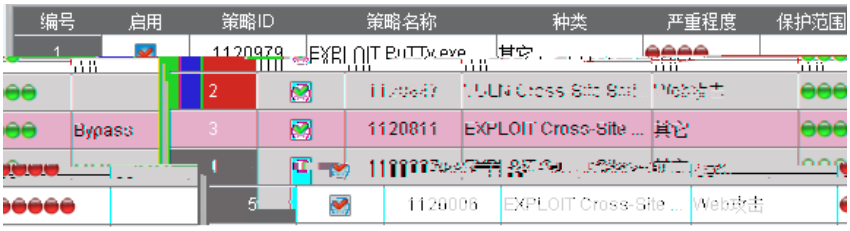

修改策略群组
策略群组名称
Security_01
入侵防御策略
病毒 / 木马防御策略
应用管理政策
Botnet防御政策
侦测政策
RBL
1130779 ET MALWARE Outeri... BotNet
1130776 ET MALWARE OutBla...
1130773 ET MALWARE OfferO...
1130770 ET MALWARE Oemji...
1130766
1130765
1130762 ET MALWARE MyWeb... BotNet
1130759 ET MALWARE MyWeb... BotNet
1130756 ET MALWARE My Sea... BotNet
BotNet
取消
确定

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
将策略赋予与策略(1120811)相同的保护范围与反应.
启用
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
预设反应
启用预设反应
确定
取消


新增保护范围与反应
确定
取消

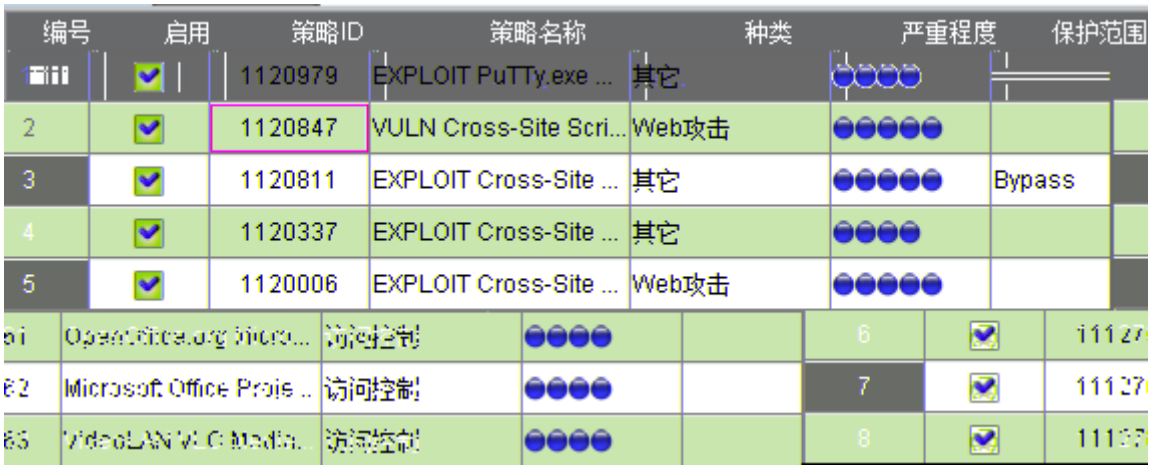

编号
启用
策略ID
策略名称
种类
严重程度
保护范围
Bypass
1120811
EXPLOIT Cross-Site ...
其它

9.7.2


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

9.8

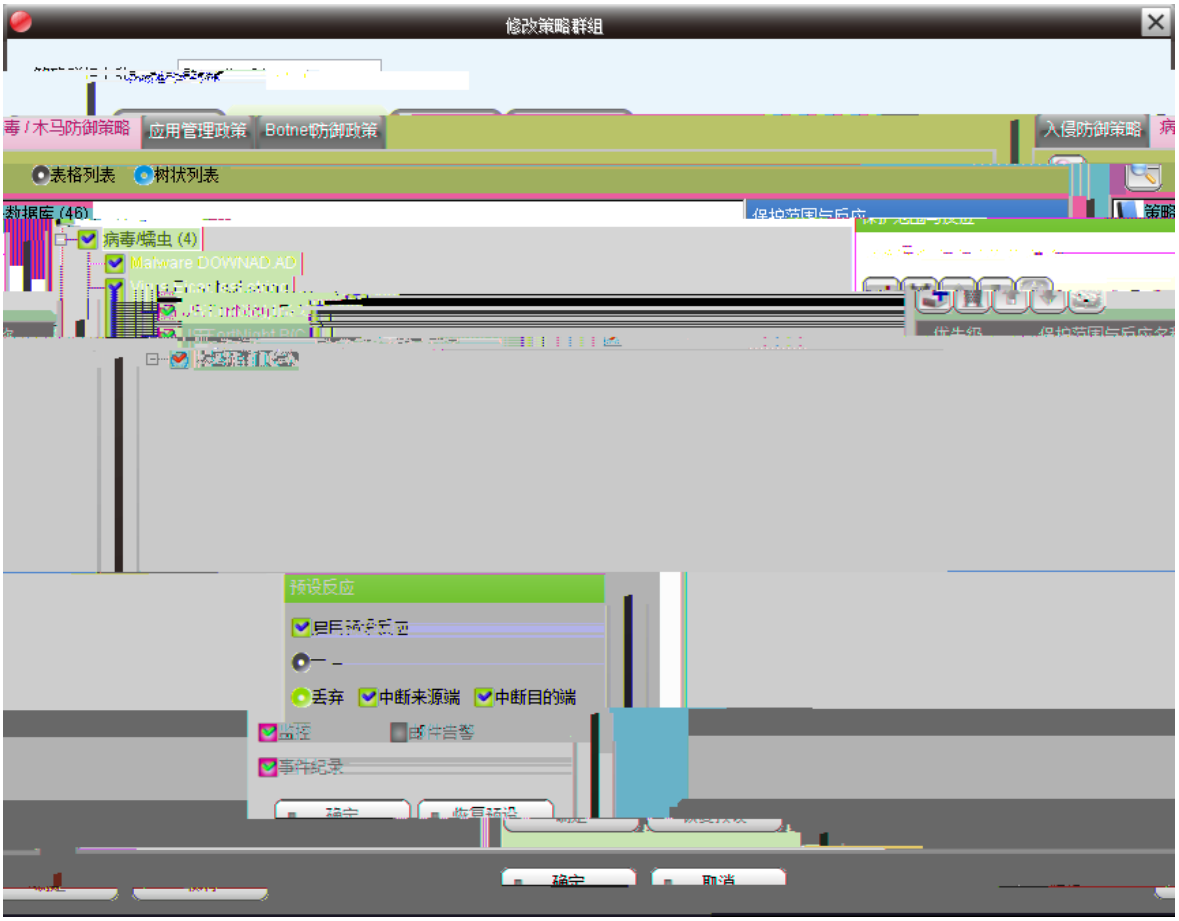
9.8.1 < >



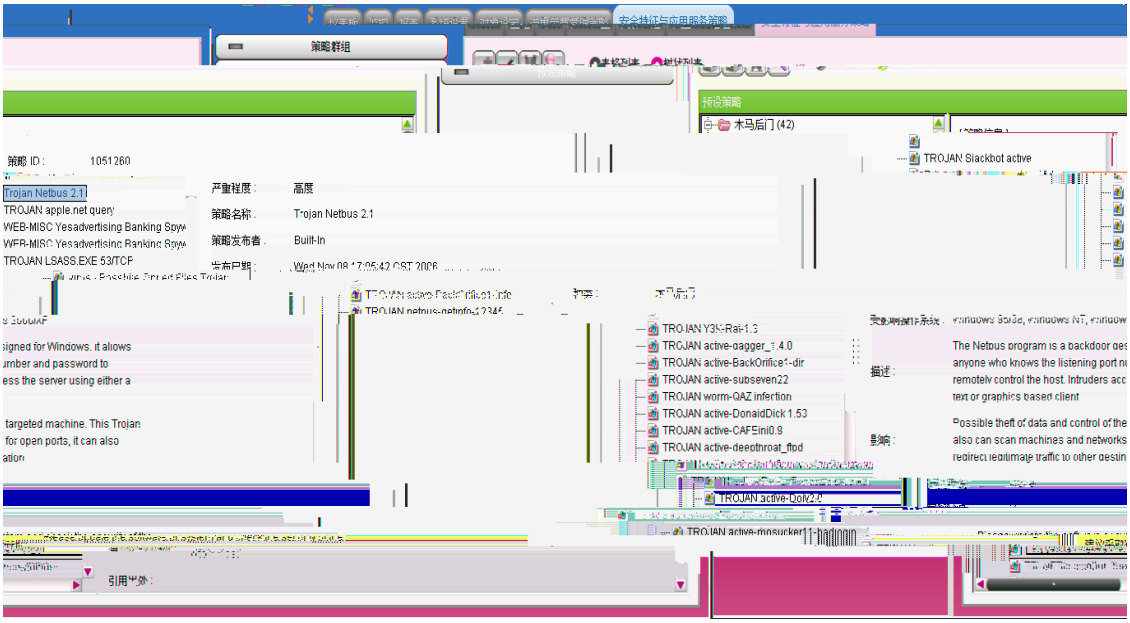
编号	启用	策略ID	策略名称	种类	严重程度	保护范围
	☑	1120979	EXPLOIT PuTTy.exe ...	其它	●●●●	
2	☑	1120847	VULN Cross-Site Scri...	Web攻击	●●●●●	
3	☑	1120811	EXPLOIT Cross-Site ...	其它	●●●●●	Bypass
4	☑	1120337	EXPLOIT Cross-Site ...	其它	●●●●	
5	☑	1120006	EXPLOIT Cross-Site ...	Web攻击	●●●●●	
81	OpenOffice.org Micro...	访问控制	●●●●	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

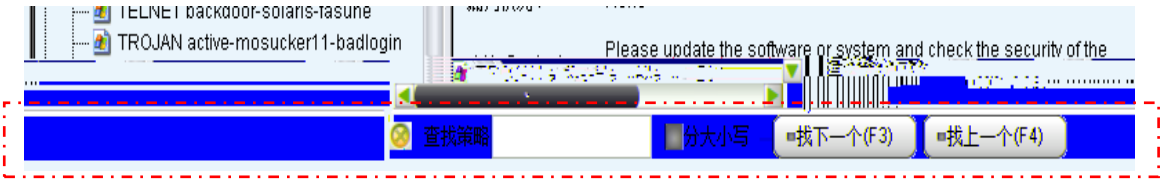
9.8.2

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)
预设反应
丢弃
中断来源端
中断目的端
事件纪录
确定
取消

9.8.5


策略群组
策略 ID : 1051260
Trojan Netbus 2.1
TROJAN apple.net query
WEB-MISC Yesadvertising Banking Spyw
WEB-MISC Yesadvertising Banking Spyw
TROJAN LSASS.EXE 53/TCP
严重程度 : 高度
策略名称 : Trojan Netbus 2.1
策略发布者 : Built-In
木马后门 (42)
TROJAN Blackbot active
TROJAN Y3K-Rat-1.3
TROJAN active-dagger_1.4.0
TROJAN active-BackOrifice1-dir
TROJAN active-subseven22
TROJAN worm-QAZ infection
TROJAN active-DonaldDick 1.53
TROJAN active-CAFEini0.9
TROJAN active-deepthroat_flod
TROJAN active-DoN2.0
TROJAN active-mosucker11-badlogin
The Netbus program is a backdoor
anyone who knows the listening port
remotely control the host. Intruders
text or graphics based client
Possible theft of data and control of the
also can scan machines and networks
redirect legitimate traffic to other
描述 :
影响 :
引用书籍 :


TELNET backdoor-solaris-tasune
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)