



RG-IDP

V1.0

©2008

Ruijie
Networks

锐捷网络

Ruijie®

锐捷

锐捷®

锐捷网络 锐捷®

Red-Giant®

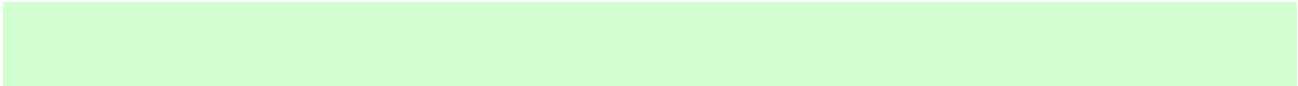
锐捷



2.



3.



Enter a

a

1+ 2
Alt A

Ctrl+Alt+A Ctrl

1		3
		3

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	

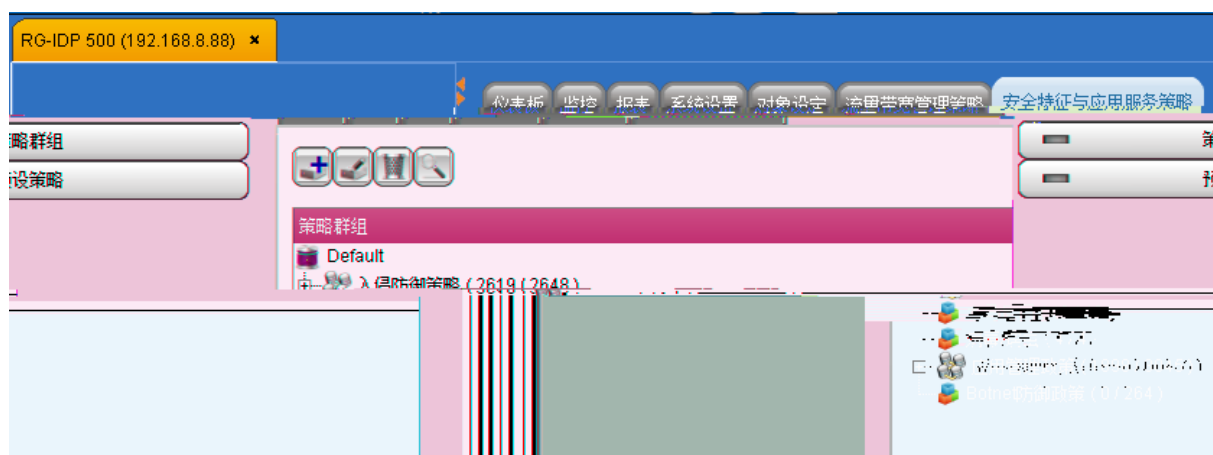
2

RG-IDP

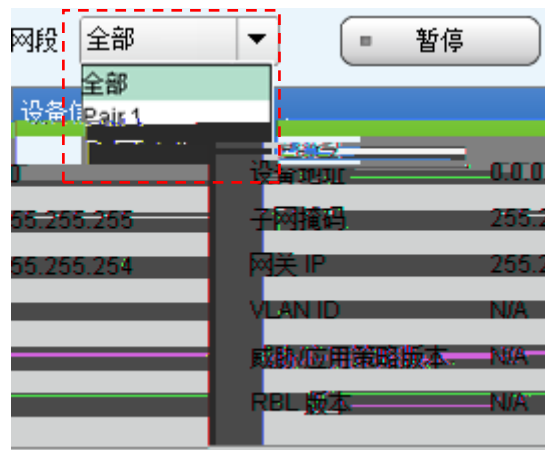
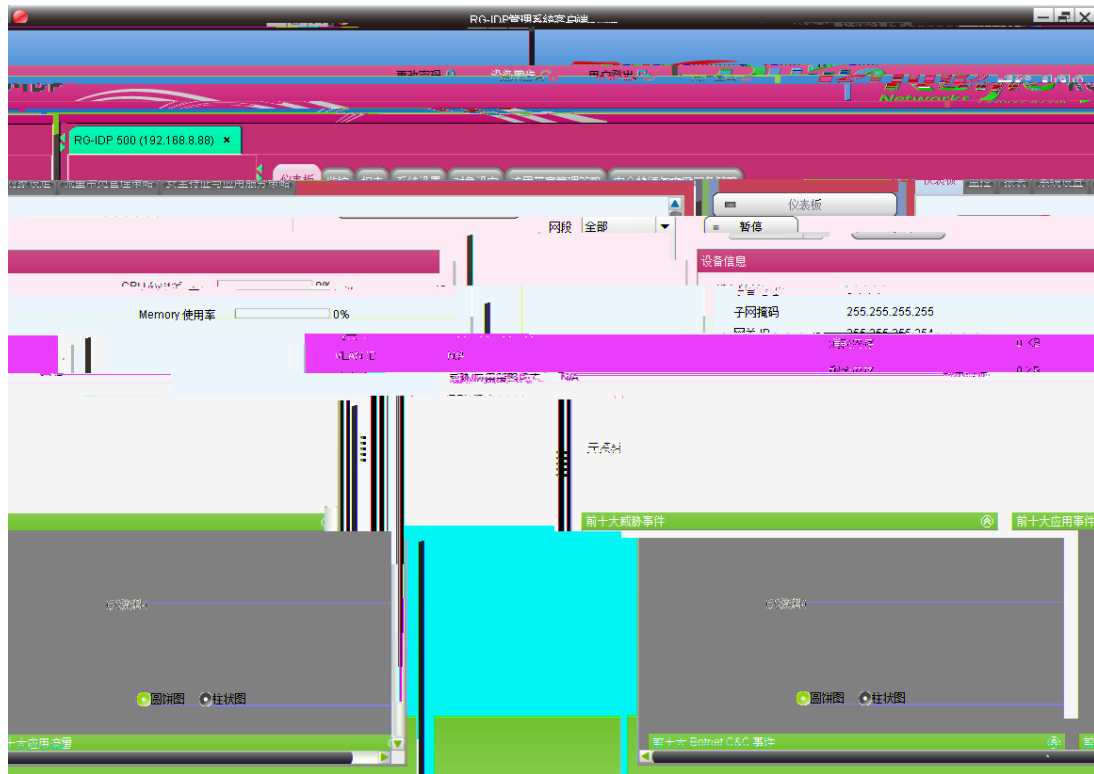
2.2

RG-IDP

2.4



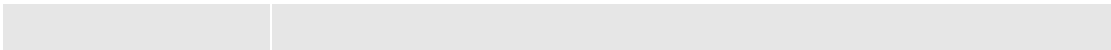
2.5



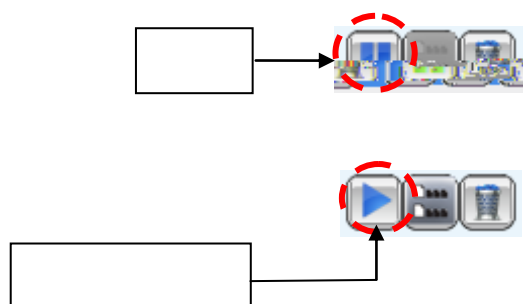
4

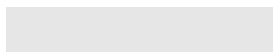
4.1





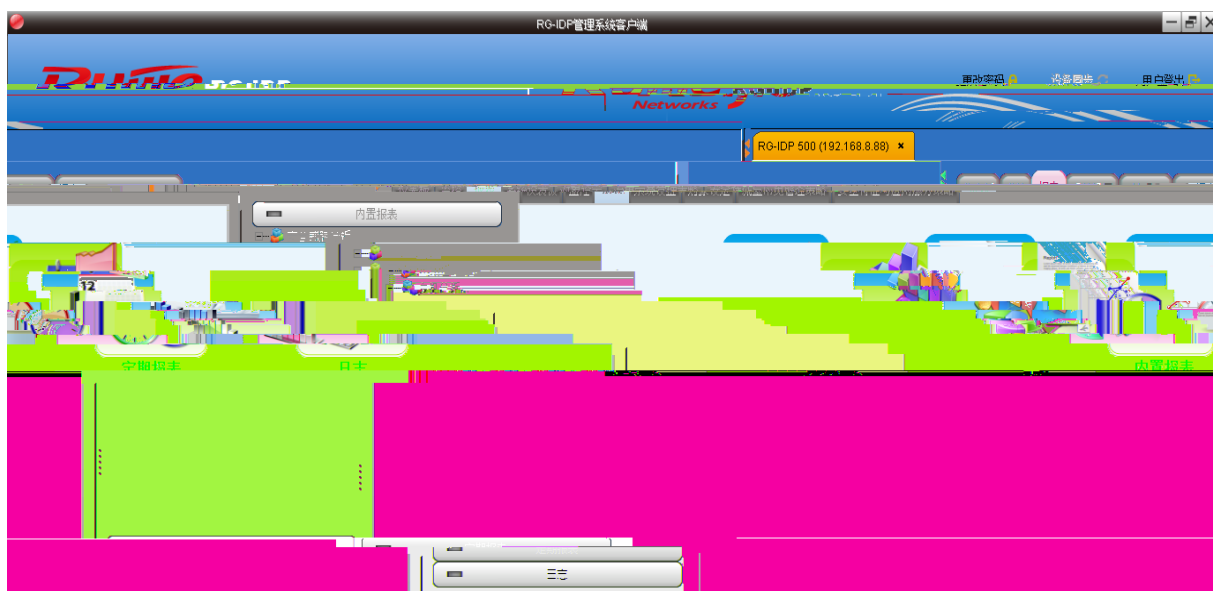
	列入流量限额黑名单 列入流量限额黑名单 流量限额使用率超过预警门坎





5

下

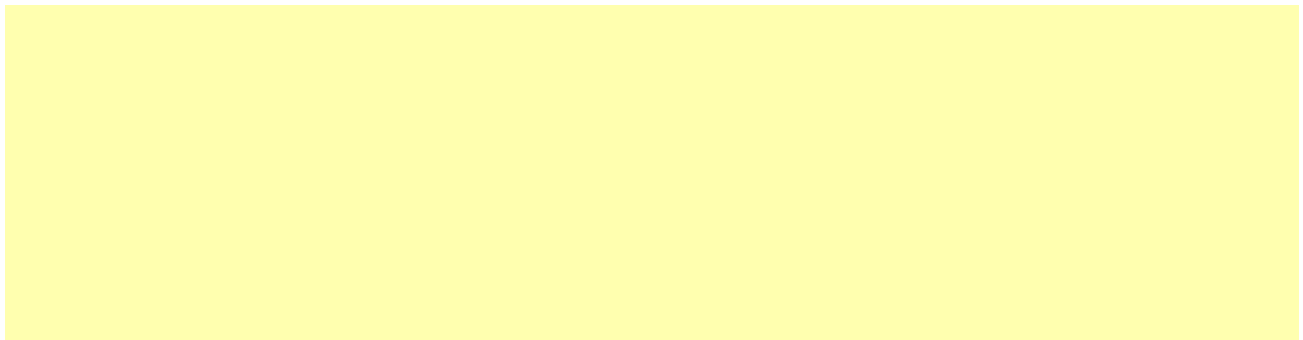


5.1 (Built-in Report)

	两

5.1.1 (Threat Analysis)

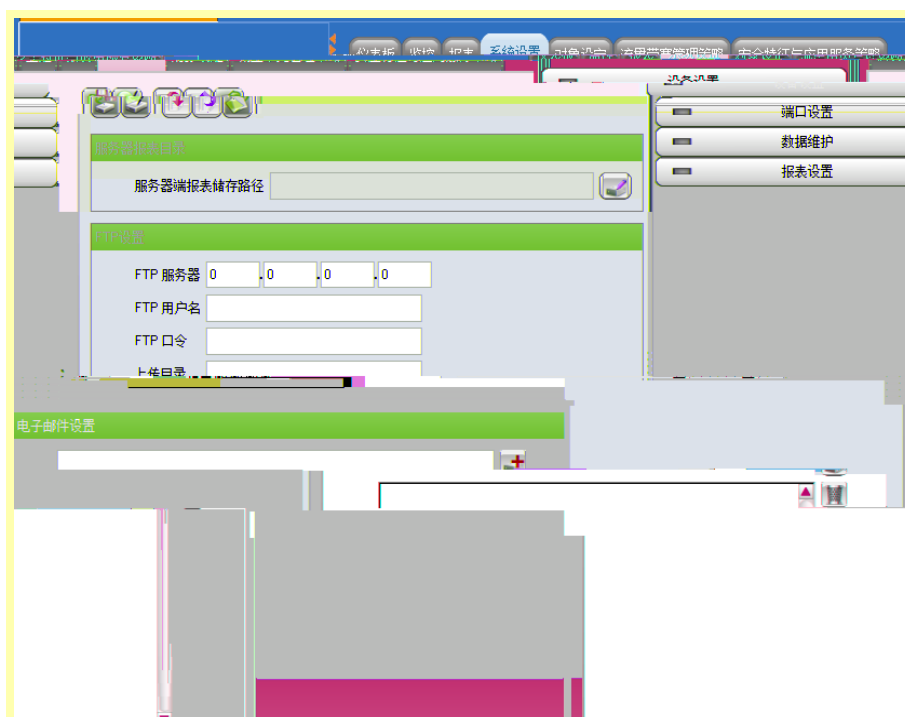
5.1.2 Botnet (Botnet Analysis)

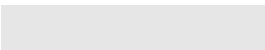


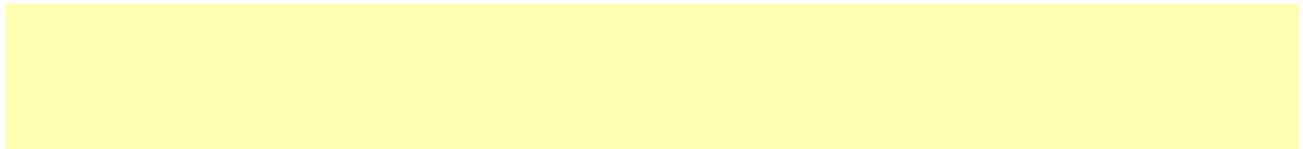
5.1.3 (Application Analysis)

RG-IDP

	两







	不
	不
	不

5.3.2 Botnet C&C

RG-IDP

5.3.6 (Blacklist)

下

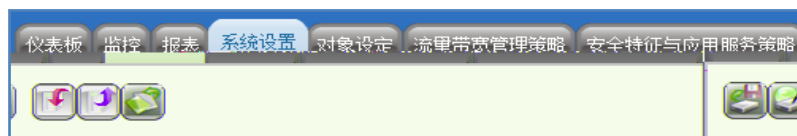


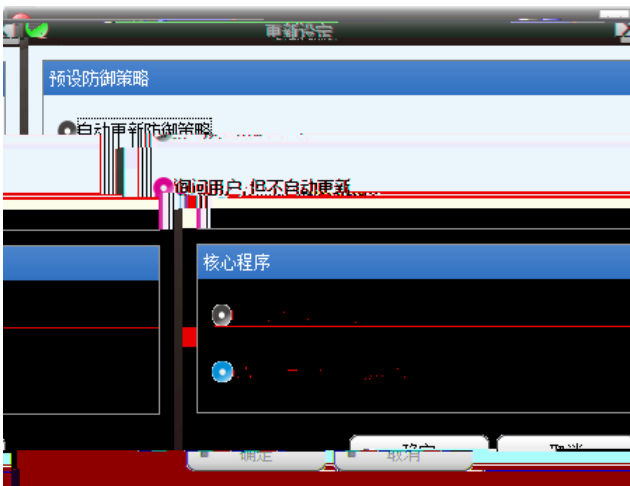
5.3.7 (System)

下

--	--

6



	两	
		
		

设备同步 

6.1 (Device Configuration)

6.1.1

全局设置

DRS IP 地址

每五秒事件记录上限

5000

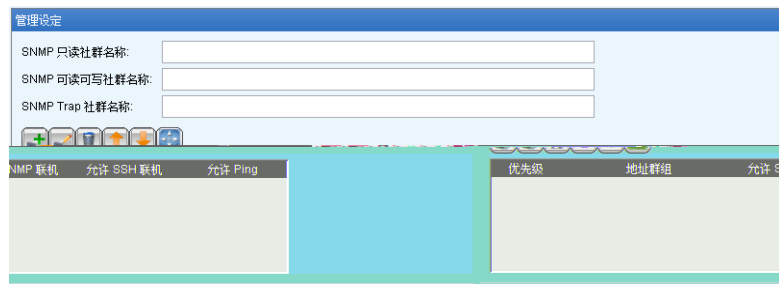
报表页面显示记录上限

10

6.1.2 (Blacklist Configuration)

6.1.3 (Device Time Information)

6.1.4 (Management Setting)



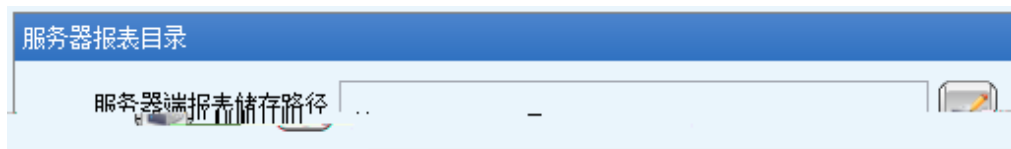
6.2



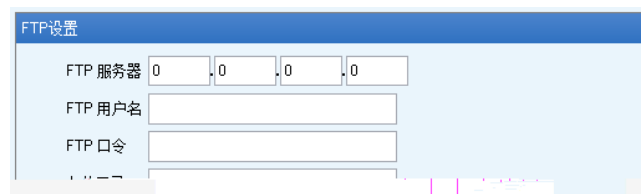


6.4

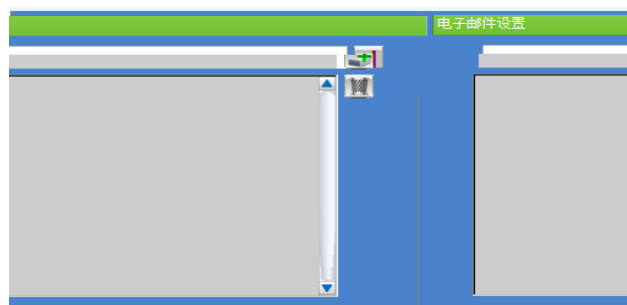
6.4.1



6.4.2 FTP



6.4.3



7



7.1

	两	
		
		

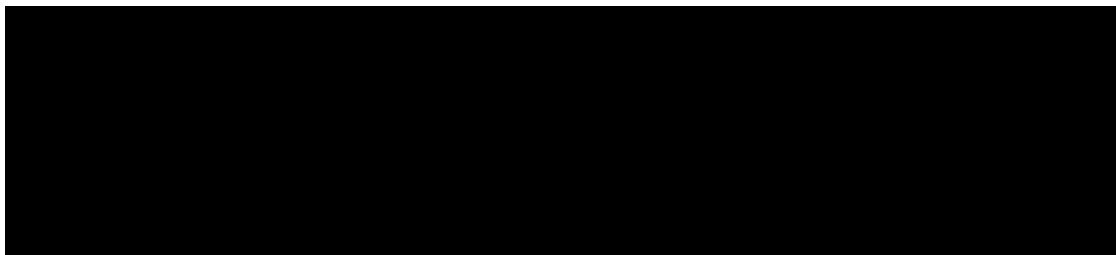
		
		

IP





7.2 VLAN

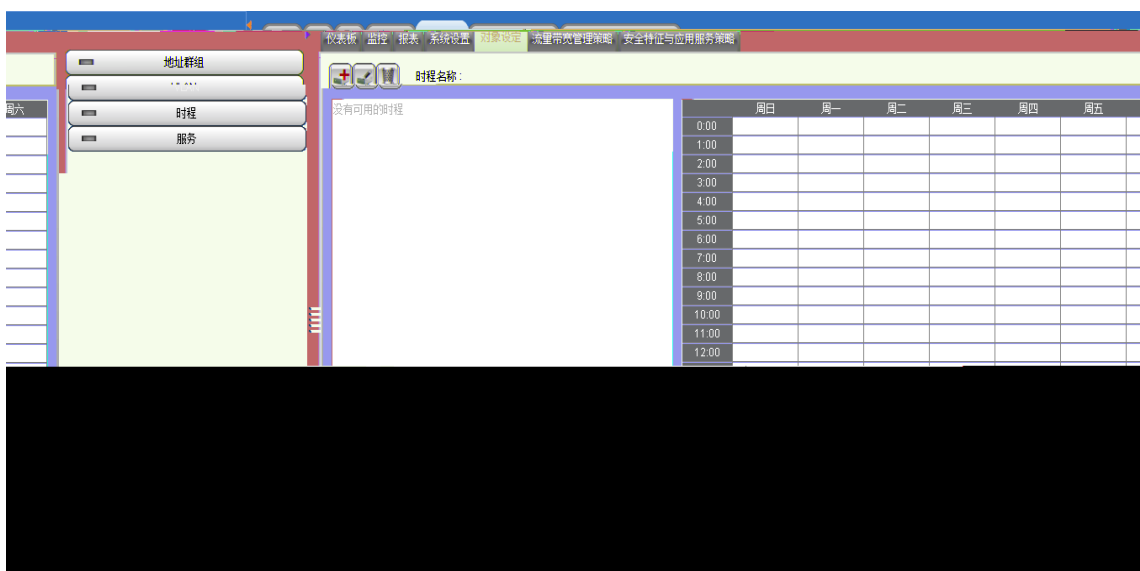


VLAN





7.3

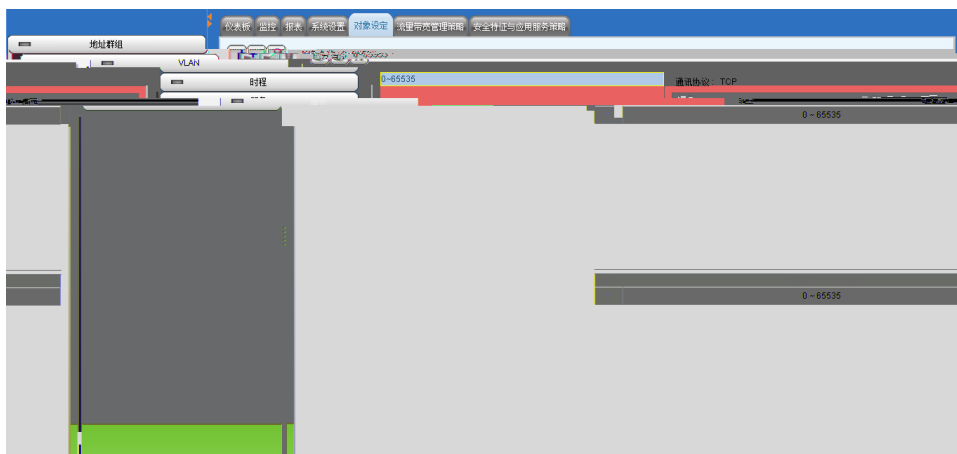


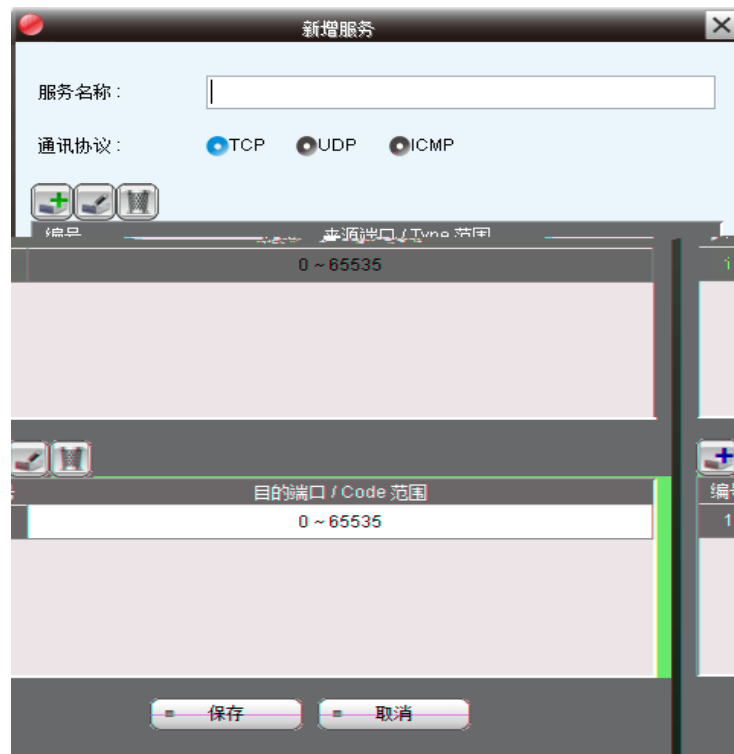
为



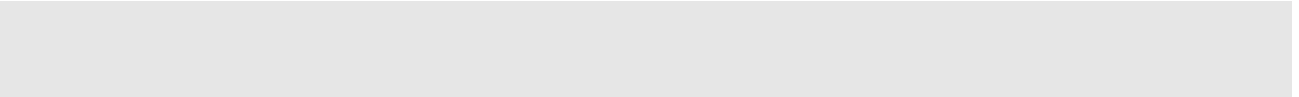
7.4

两





8

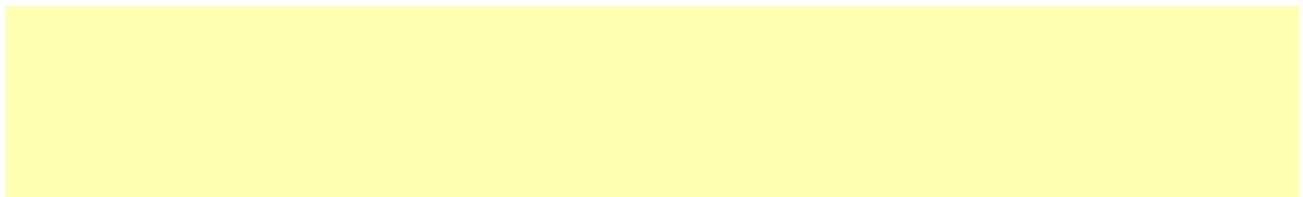
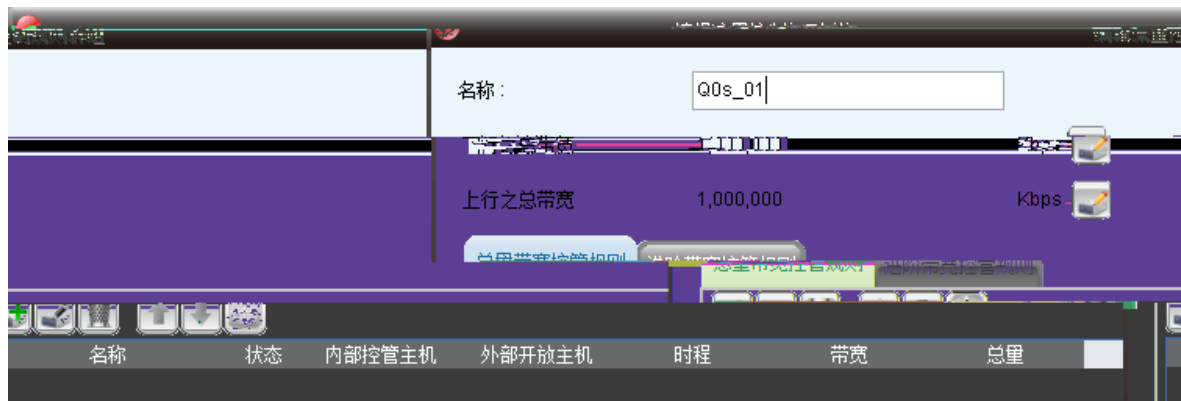


8.2.1



8.2.2



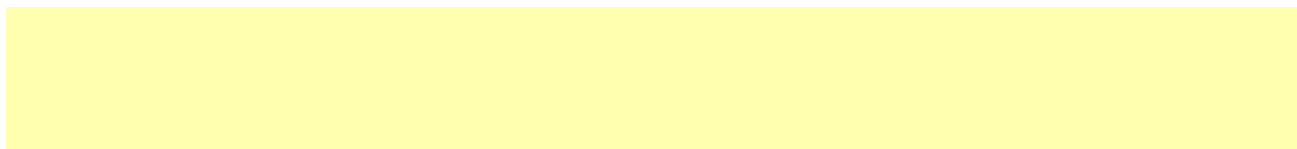


	两	
		
		
		
		
		
		



8.3.1

比对条件	
内部控管主机	ANY_HOST
外部开放主机	N/A



8.3.2

--	--

两

	两	
		
		
		
		
		
		

8.4.1

基本设定

名称：

QoS_01

层：

1

100%

100%

8.4.2

8.4.3

9

9.1.1

两

9.1.2

9.1.3 Botnet

9.2

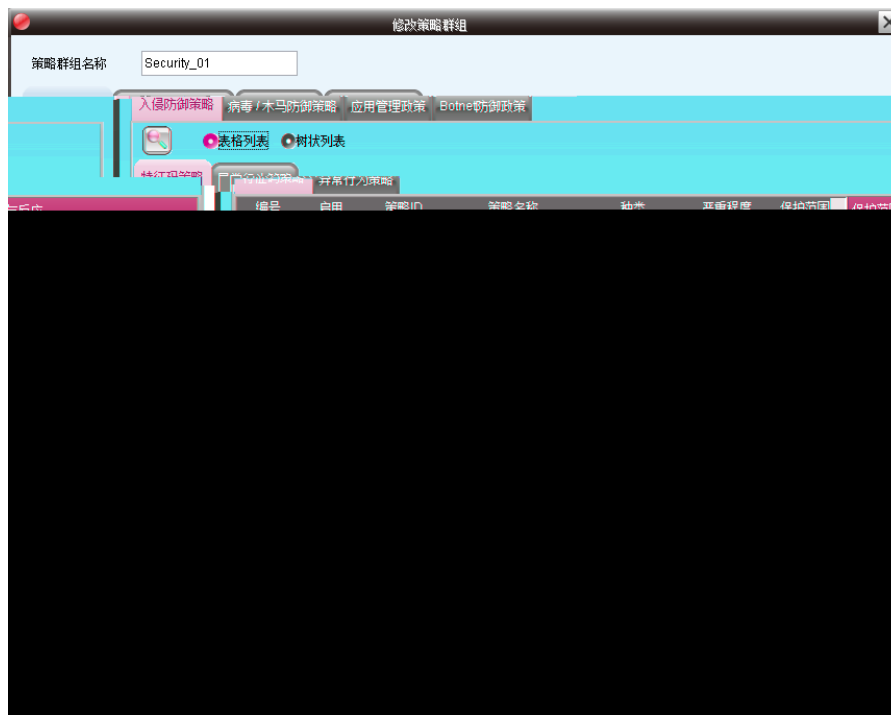
RG-IDP

9.2.4

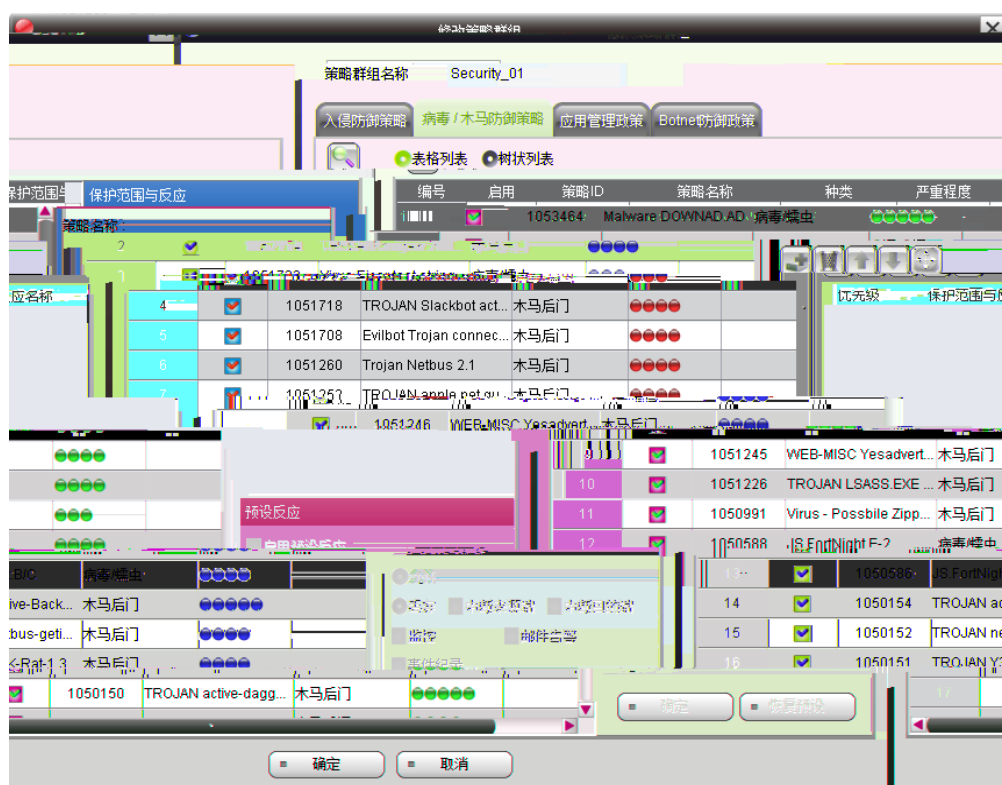
9.3

9.3.2

9.3.3

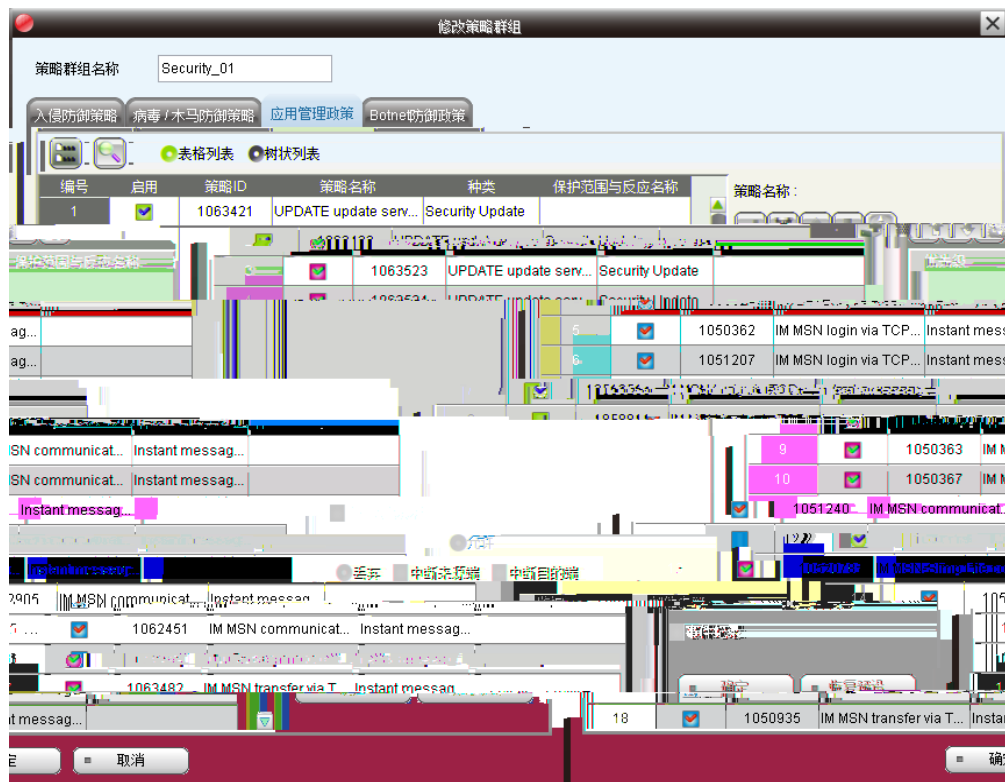


9.3.4



9.5





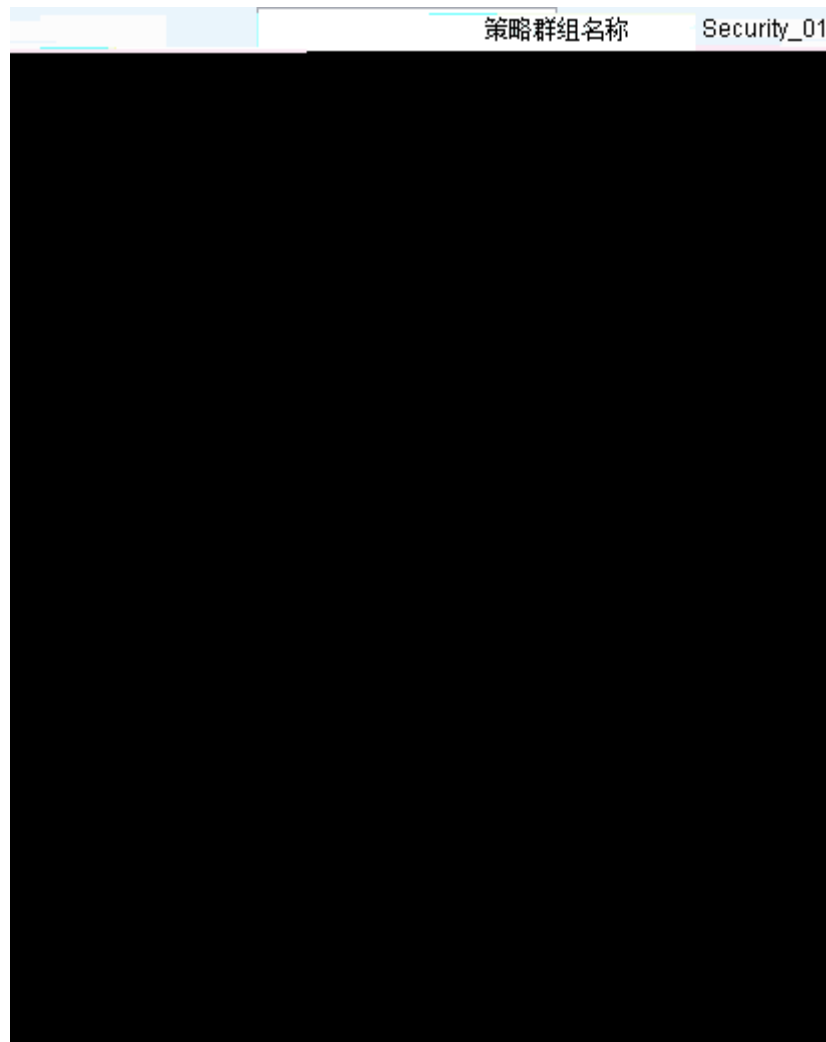
9.5.1



两

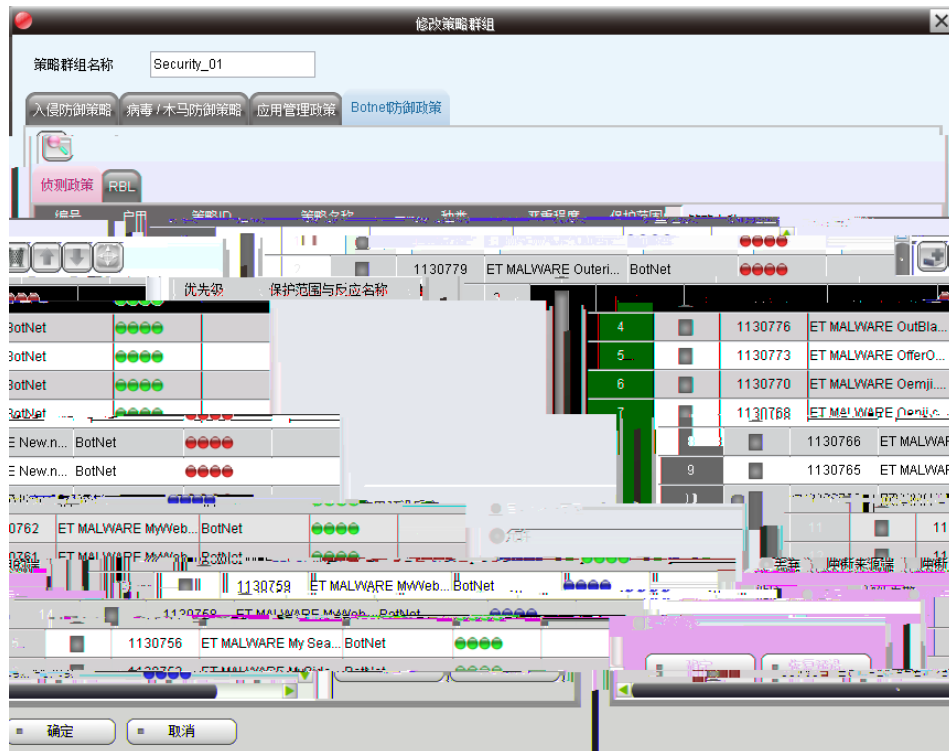


9.5.3



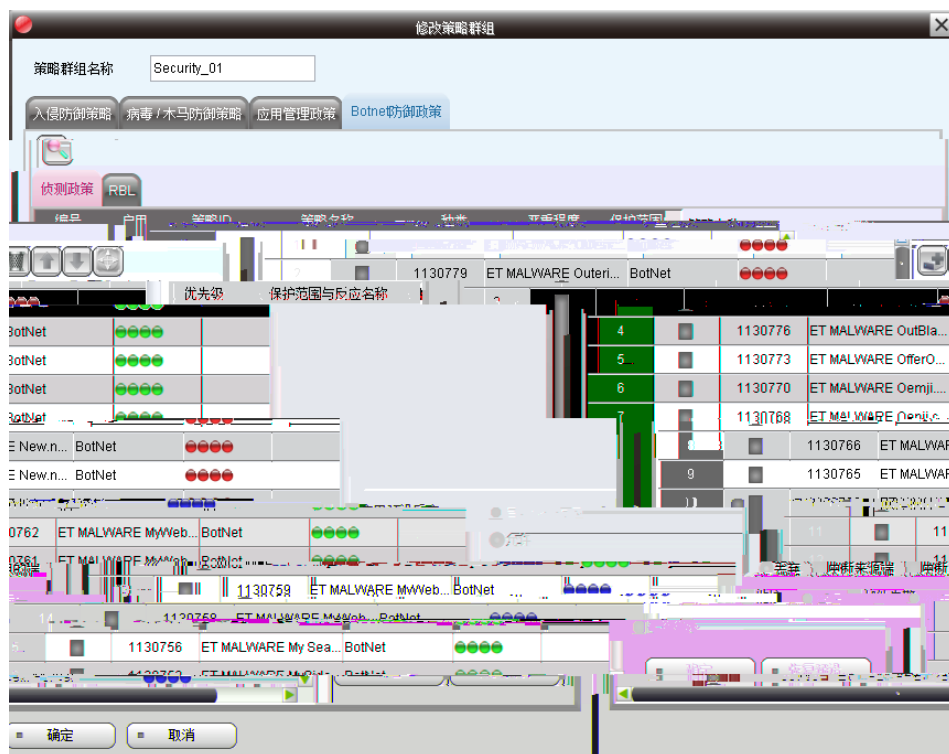
9.6 Botnet





下

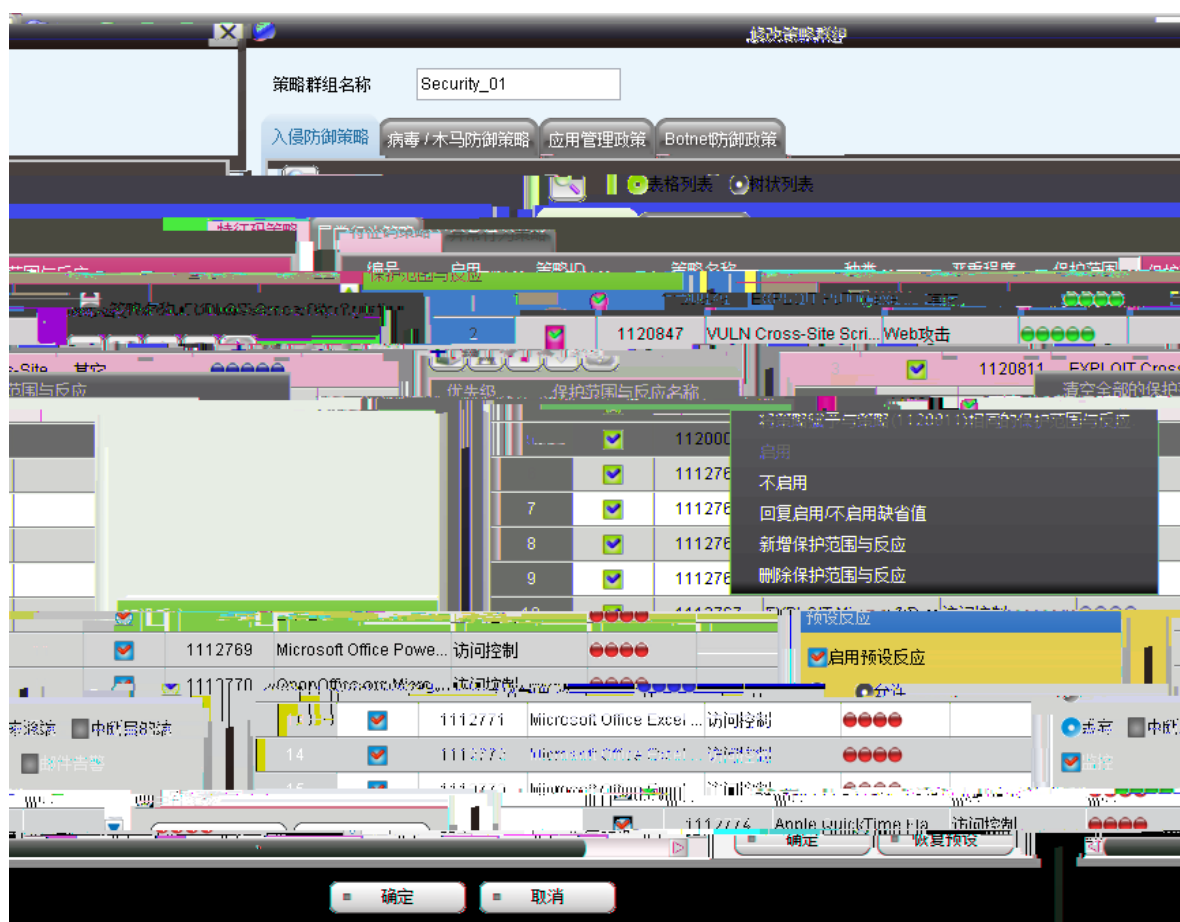
9.6.1



9.6.2 RBL



9.7.1



两



新增保护范围与反应

名称

保护范围

☒ 来源主机

☒ 目的主机

☒ VLAN 群组

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 取消

[illegible]

编号	启用	策略ID	策略名称	种类	严重程度	保护范围
1		1120879	EXPLOIT PuTTY.exe	其它		
Web攻击						
其它		Bypass				
1						
Web攻击						

两

两

9.7.2

两

两

两

两

两



9.8

9.8.1

<

>

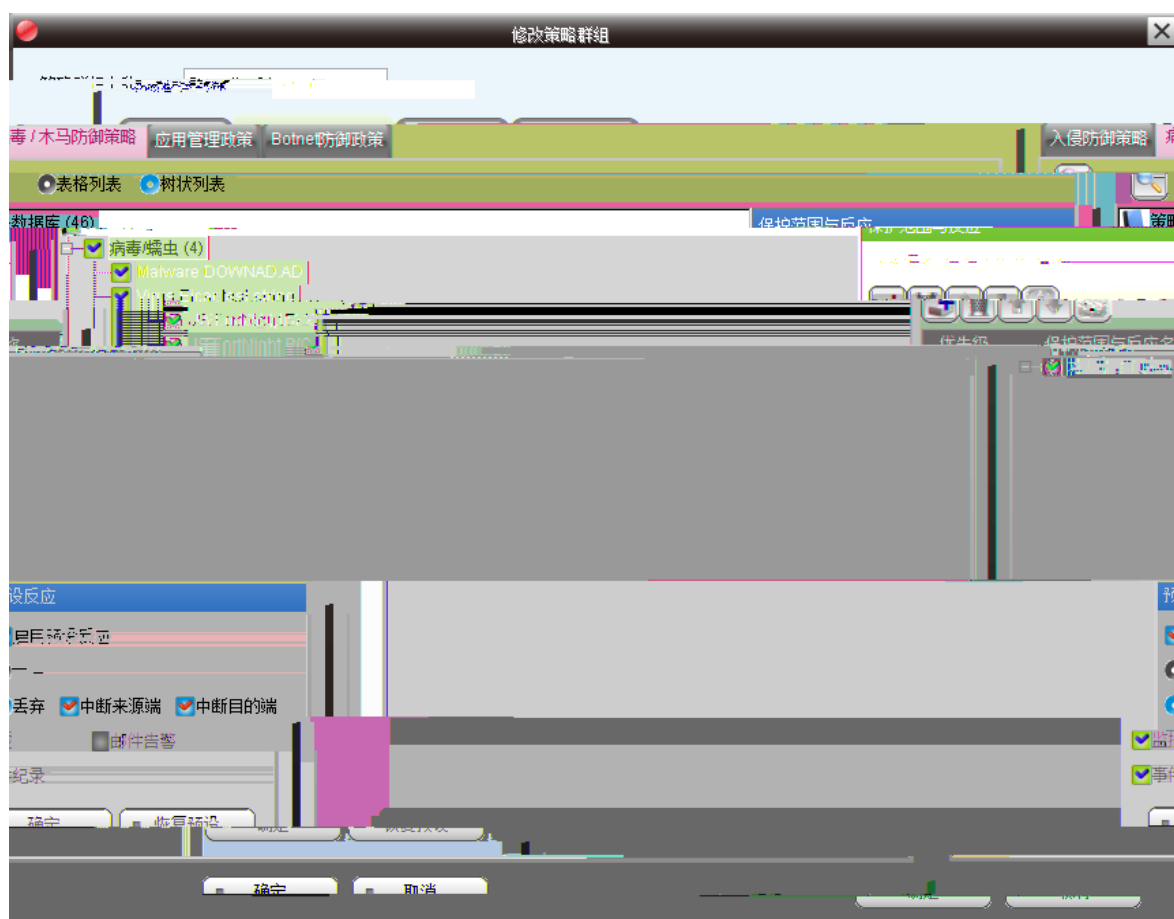


编号	启用	策略ID	策略名称	种类	严重程度	保护范围
	☒	1120979	EXPLOIT PuTTY.exe ...	其它		
2	☒	1120847	VULN Cross-Site Scri...	Web攻击		
3	☒	1120811	EXPLOIT Cross-Site ...	其它		Bypass
4	☒	1120337	EXPLOIT Cross-Site ...	其它		
5	☒	1120006	EXPLOIT Cross-Site ...	Web攻击		
61		OpenOffice.org Micro...	访问控制		6	☒
62		Microsoft Office Prois ...	访问控制		7	☒
65		VideoLAN VLC Media...	访问控制		8	☒

9.8.2



9.8.4



9.8.5

