

RG-WG WebGuard

V3.50.2.40r6

5.1.4		54
5.1.5		55
5.1.6	WEB	56
5.1.7	WEB	56
5.1.8		57
5.1.9		58
5.1.10		60
5.1.11	IP		

7.1.7	112
7.2	116
7.2.1	116
7.2.2	119
7.2.3	MAC	121
7.2.4	ARP	122
7.2.5	123
7.2.6	125
7.3	132
7.3.1	132
7.3.2	138
7.3.3	138
7.3.4	139
7.4	140
7.4.1	

1

1.1

WebGuard	(RG-WG)	WEB
HTTP/HTTPS		
WEB	WEB	
WEB2.0		
	WEB	WEB
		SQL

1.2

WEB

RG-WG WebGuard

RG-WG WebGuard

1.3

www.ruijie.com.cn

4008111000.

" "

2

RG-WG HTTPS WEB
(CLI) CLI RG-WG
RG-WG



WEBUI CLI CLI
" "

WEBUI

2.2 WEBUI

WEBUI

>



WEBUI

•

•

- WEB URL " " URL
DoS WEB Webshell

管理 > 访问管理 > 访问控制

空闲超时值	<input type="text" value="30"/>	(5-30)分钟
登录重试次数	<input type="text" value="5"/>	(0-10)次
锁定时间	<input type="text" value="5"/>	(5-30)分钟
HTTPS端口	<input type="text" value="443"/>	
SSH端口	<input type="text" value="22"/>	

管理主机

3

3.1

	"
CPU	CPU

" "

3.2

>

HTTP

HTTPS

Web

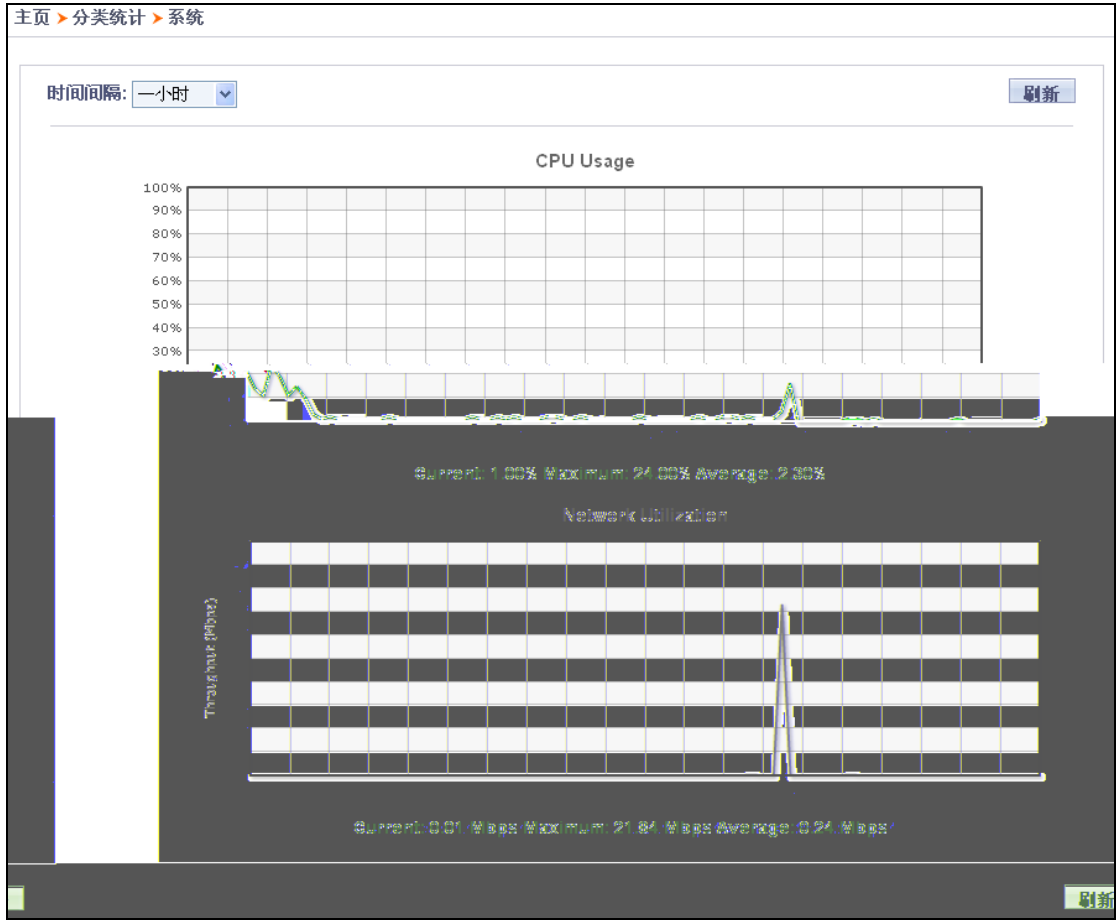
WEB

3.2.1

>

>

CPU



" CPU " CPU

CPU

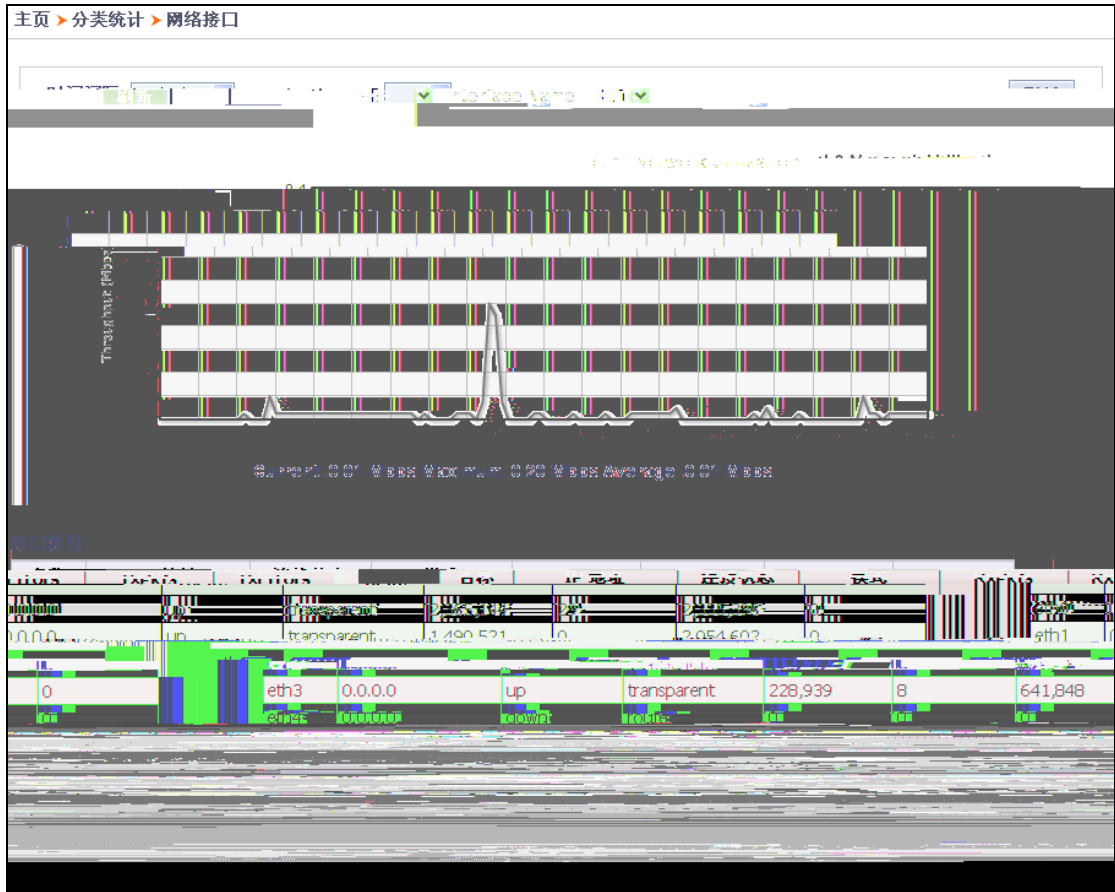
" "

" "

" "

3.2.2

> >



IP	IP 0.0.0.0
	" up" " down" vlan1 vlan1 vlan1 vlan1
	" " " "
Rx Pkts	
Rx Errors	

" "

00 01

00 01

7

1 00 01

30

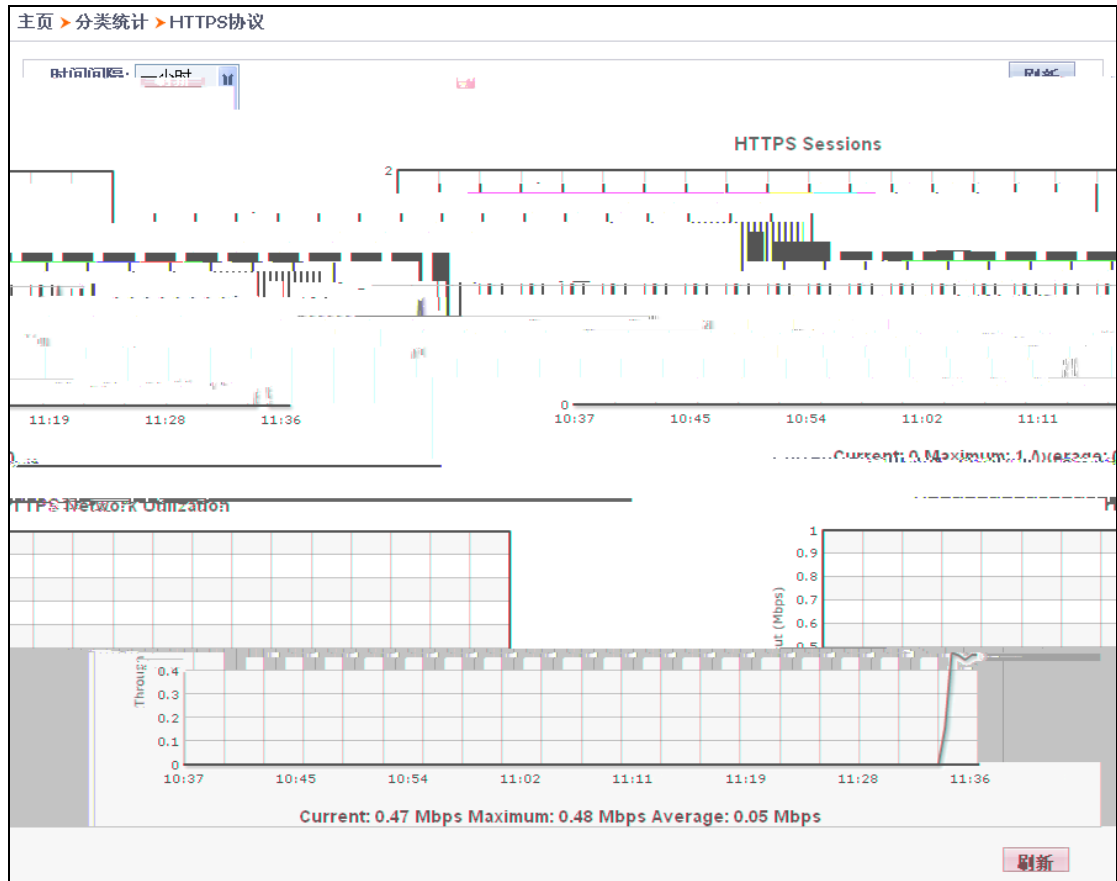
30

" "

" "

3.2.4 HTTPS

HTTPS > HTTPS 1



" "

00 01

00 01

7

1 00 01

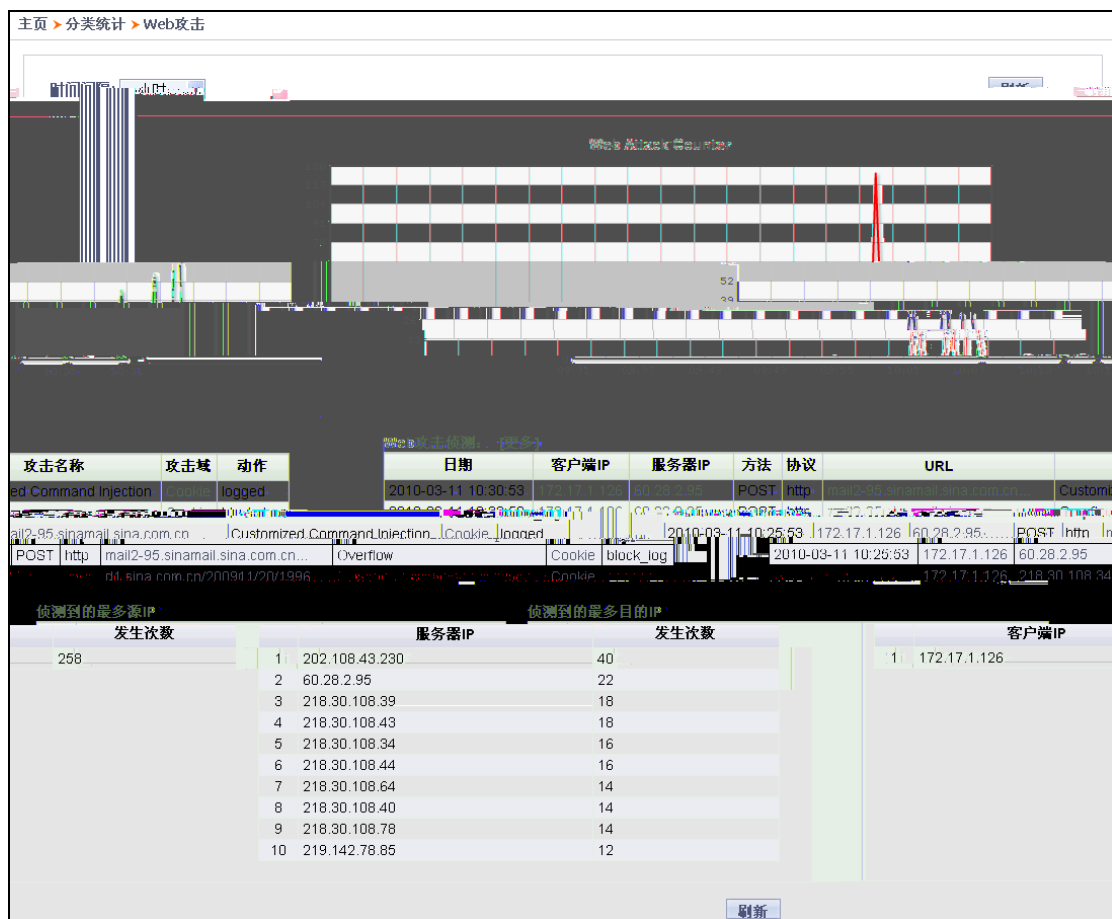
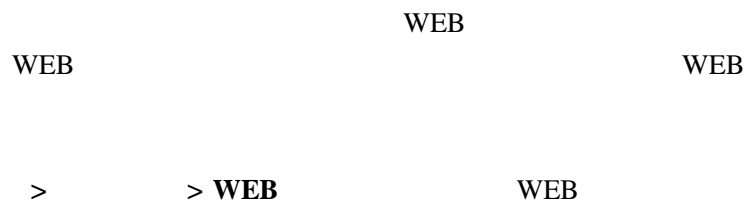
30

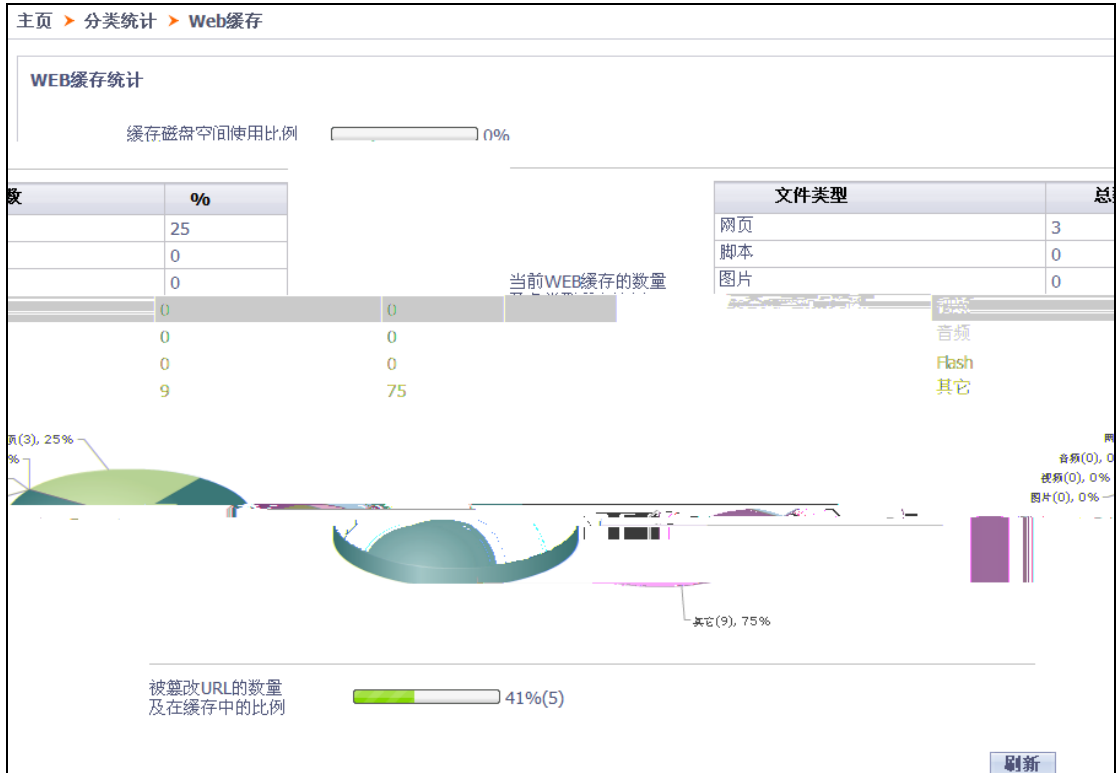
30

“ ”

“ ”

3.2.5 WEB





"

"

"

WEB

"

4

WEB

WEB

WEB

4.1

RG-WG

	CPU
	N
	N
	N

PC

4.1.1

" "

1 > >

报表和日志 > 报表 > 已生成报表

每页显示 25 K < > X 总页数: 1 页号: 1 翻到

<input type="checkbox"/>	生成日期/时间	报表类别	导出
<input type="checkbox"/>	2010-02-05 10:35:11	攻击报表	
<input type="checkbox"/>	2010-02-05 10:35:11	访问报表	
<input type="checkbox"/>	2010-02-05 10:35:11	病毒报表	
<input type="checkbox"/>	2010-02-05 10:35:11	综合报表	
<input type="checkbox"/>	2010-02-05 10:35:01	访问报表	<input type="checkbox"/> 2010
<input type="checkbox"/>	2010-02-05 10:35:01	病毒报表	<input type="checkbox"/> 2010
<input type="checkbox"/>	2010-02-05 10:32:55	综合报表	<input type="checkbox"/> 2010
<input type="checkbox"/>	2010-02-05 10:32:55	攻击报表	<input type="checkbox"/> 2010
<input type="checkbox"/>	2010-02-05 10:32:55	访问报表	<input type="checkbox"/> 2010
<input type="checkbox"/>	2010-02-05 10:32:55	病毒报表	<input type="checkbox"/> 2010

删除

K < > X 总页数: 1 页号: 1 翻到

2

3	"	"	PC
4	"	"	

4.1.2

7.1.4

1 > >



报表和日志 > 报表 > 定制生成报表

显示过去30天的数据)
至多只显示过去30天的数据)
过去30天的数据)

攻击事件时间分布图
攻击类型比例图
服务器IP地址事件排名

报告:

- 综合报表
 - 网络流量(至多只)
 - CPU/内存使用率)
 - 会话(至多只显示

病毒报

IP地址

所有
选定: 服务器范围(掩码): 0.0.0.0/0
选定: 安全组:

计划时间:
 每天
 每星期
 星期天

对生成的报表的操作:
 本地保存
 邮件发送 语言: English

报表将会发送给在下面页面中设置的帐户:
管理 -> 系统设置 -> 邮件配置

应用 取消

B " from" " to"

5 " " "

4.2

> > >

1 [7.1.2.3](#)

2 " " UTF-8
>

4.2.1

Web

SQL

WEB

WEB

WebShell

IP WEB

WEB URL URL POST Cookie

WEB

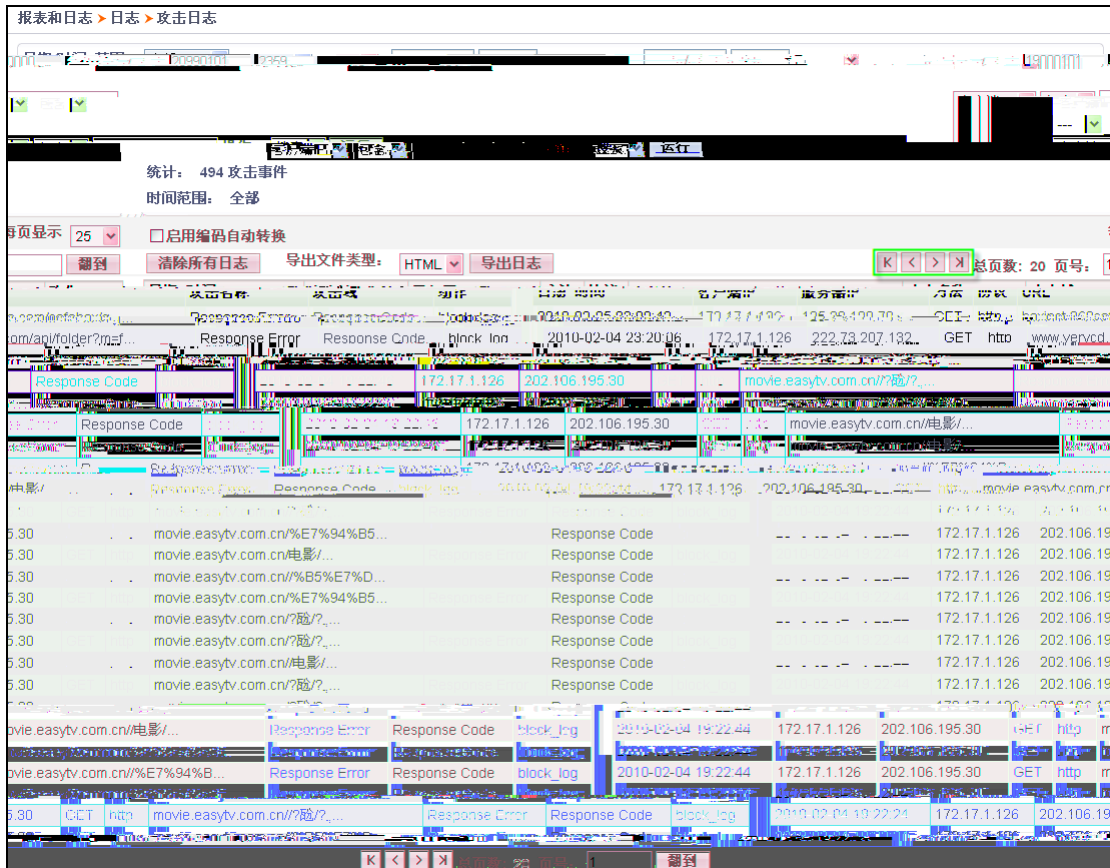
IP WEB

Cookie

http

1

> >



"

>

"

25

2



B " "

" " "

" "

" "

C " "

" " "

D " "

" "

" "



4.2.2

" " WEB

1 > >

B " "

"

" " "

" "

" "

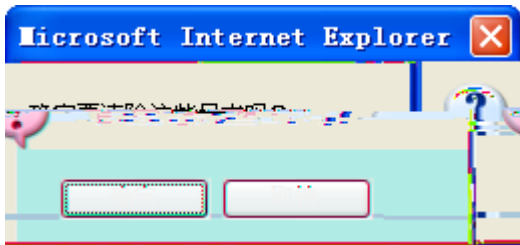
C " " " "

"

D " "

" "

" "



4.2.3

WEB

1

> >

IP	WEB IP
	WEB GET URL POST
URL	URL
	WEB

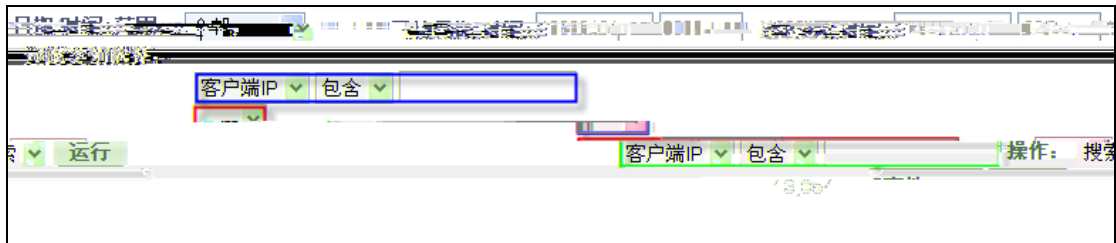
3 " "

4 PC " "

HTML CSV " "

5

IP IP



A " / "

" " 00:00:00

" " 00:00:00

" 7 "

" " 1 00:00:00

" 30 " 30

" " " / " " / "

1

B " "



报表和日志 > 日志 > 管理 > 系统日志

日期 时间 范围 全部 开始日期时间 20091201 结束日期时间 20091201 2009

统计: 647 系统事件
时间范围: 全部

每页显示 25

HTML 导出日志

日期	时间	系统事件
2009-12-31	18:34:00	Adjust time from NTP server 72.14.179.211 offset 0.024885 sec
2009-12-31	15:11:03	Adjust time from NTP server 72.14.179.211 offset 0.024885 sec
2009-12-31	12:48:07	Adjust time from NTP server 198.144.194.12 offset 0.037831 sec
2009-12-31	10:29:07	Adjust time from NTP server 207.171.114.81 offset 0.028274 sec
2009-12-31	12:12:07	Adjust time from NTP server 72.167.54.201 offset 0.024298 sec

总页数: 26 页号: 1

" "

>

" "

25

" "

" "

" "

2

3 " "

4 PC " "

HTML CSV " "

5

IP IP

日期/时间 范围: 开始日期/时间 结束日期/时间

过滤类别选择:

操作:

统计: 647 系统事件

A " / "

" " 00:00:00

" " 00:00:00

" 7 "

" " 1 00:00:00

" 30 " 30

" " " / " " / "

1

B " "

" " "

" "

" "

C " "

"

D " "

" "

" "



5 WEB

WEB

URL

WEB

	WEB
SQL	SQL WEB SQL
	XSS
	WEB
	WEB
	WEB
	WEB 500 1024
WEB	RG-WG
Webshell	WEB Webshell
WEB	WEB RG-WG

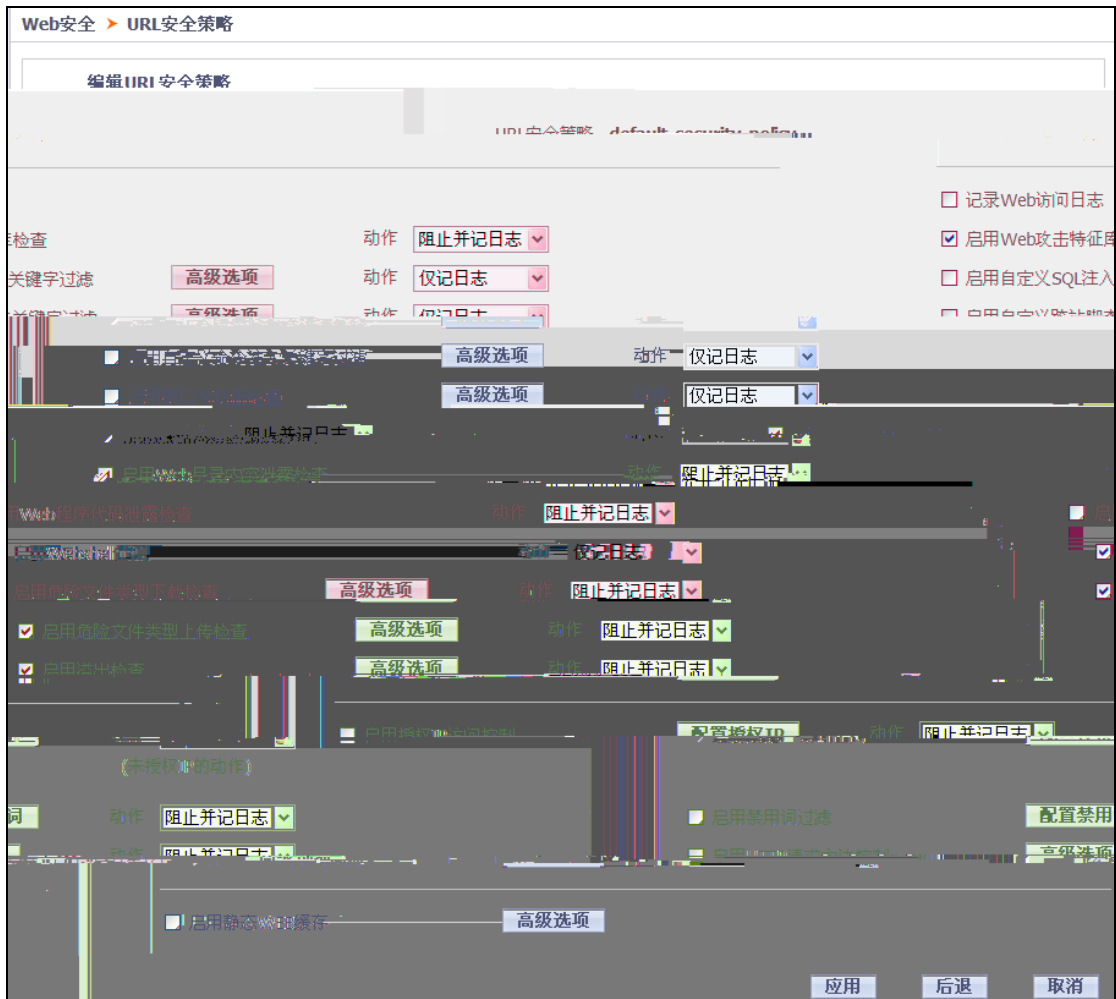
WEB

...

c " " " " URL

3

" " " "

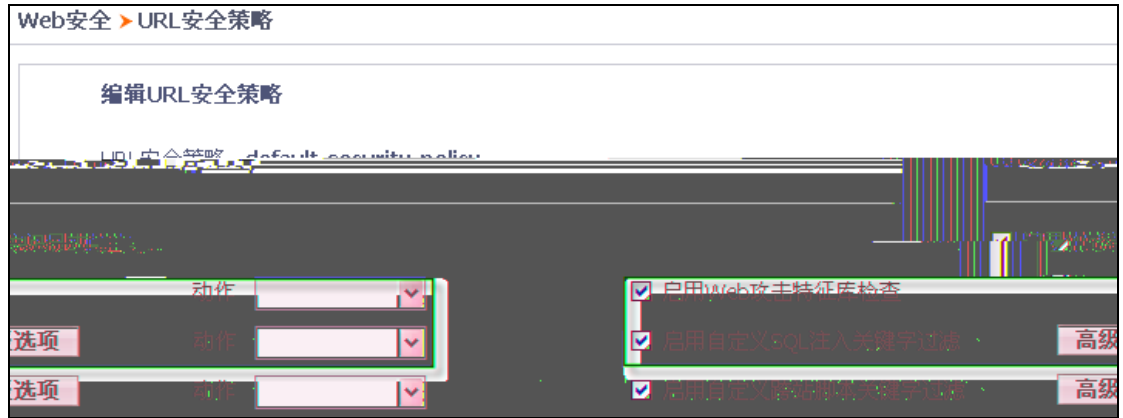


4 URL

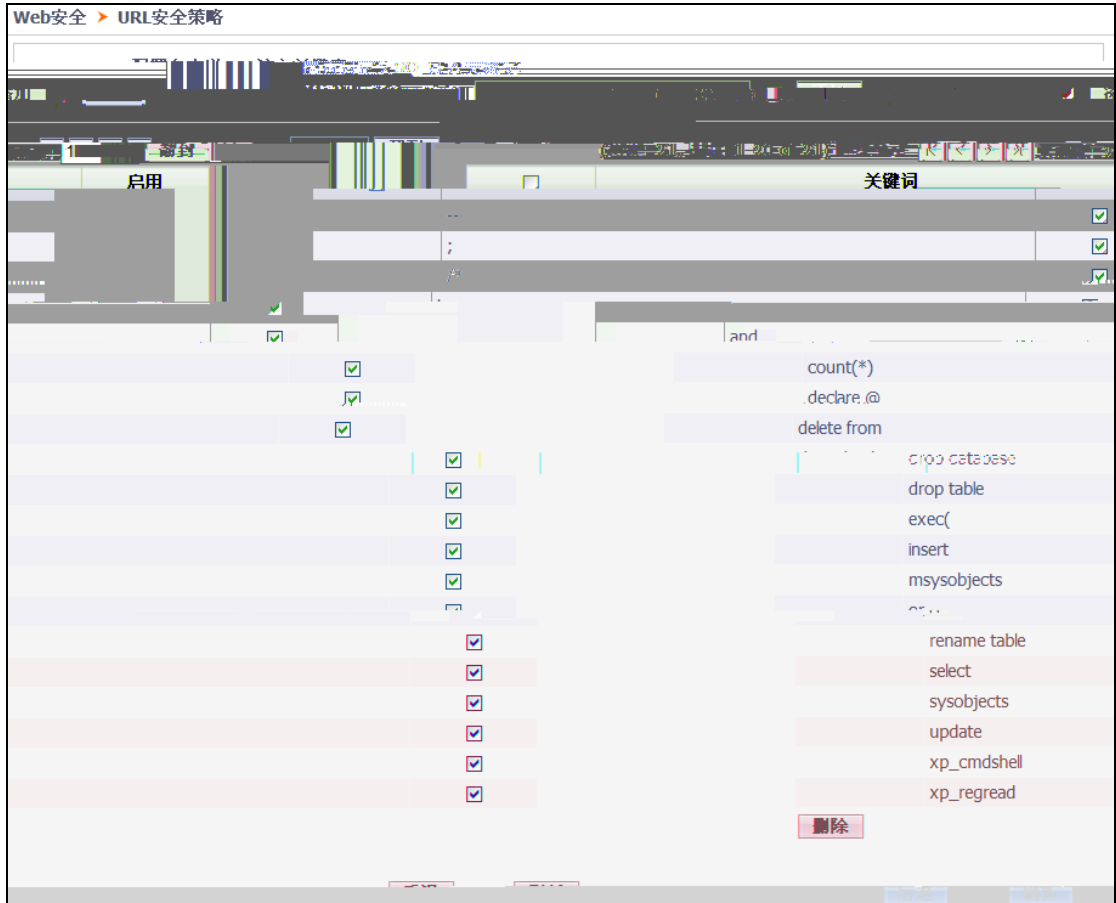
RG-WG

URL

" "



1	"	Web	"	"
SQL	"	"	"	"
2	"	SQL	"	WEB
SQL	"	"	"	"
3	"	"	SQL	"



" " SQL

A

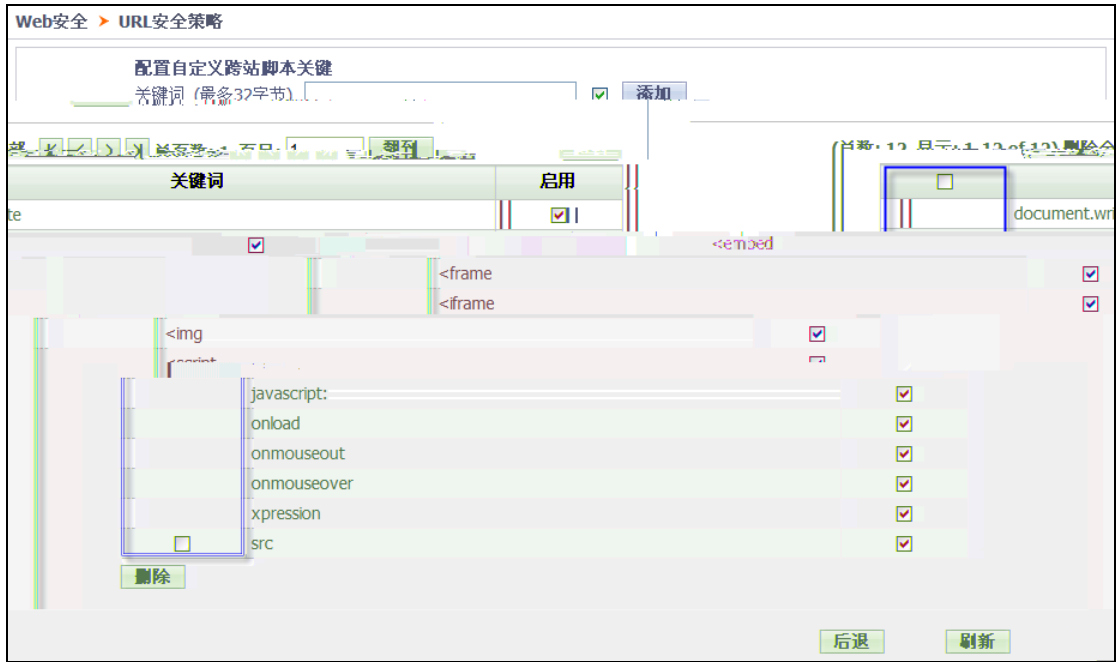
A Web

,
B

CGI

HTML
Cookie

RG-WG



B

" "

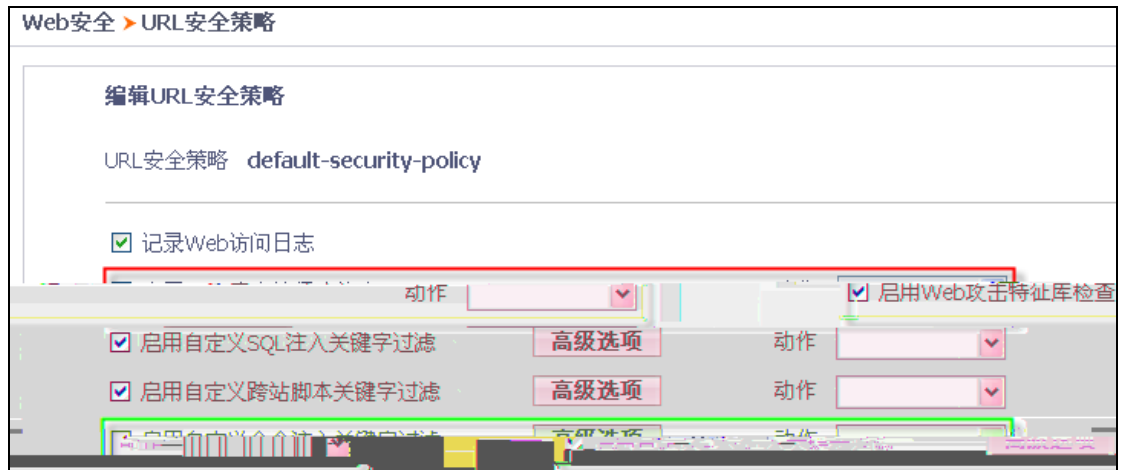
5.1.3

HTML

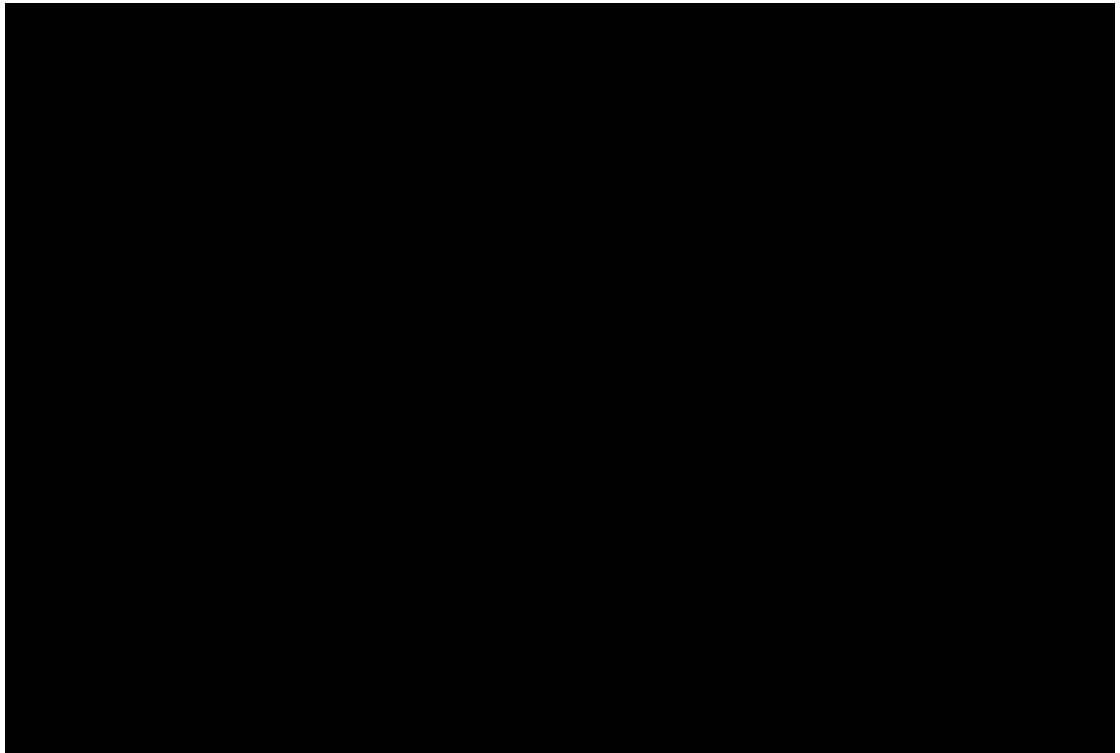
()

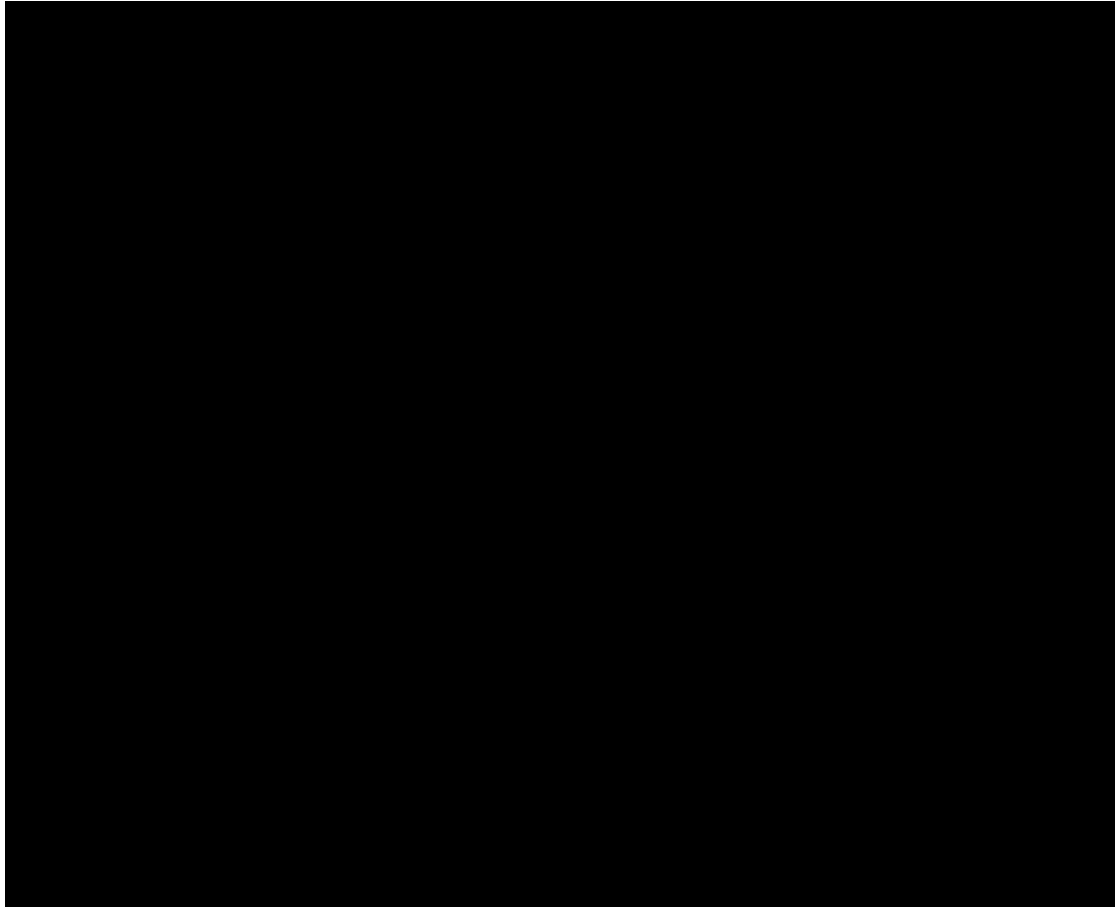
RG-WG

URL



- 1 " Web " "
- 2 " "
- 3 " "





" "

" "

5.1.5

WEB

RG-WG

WEB



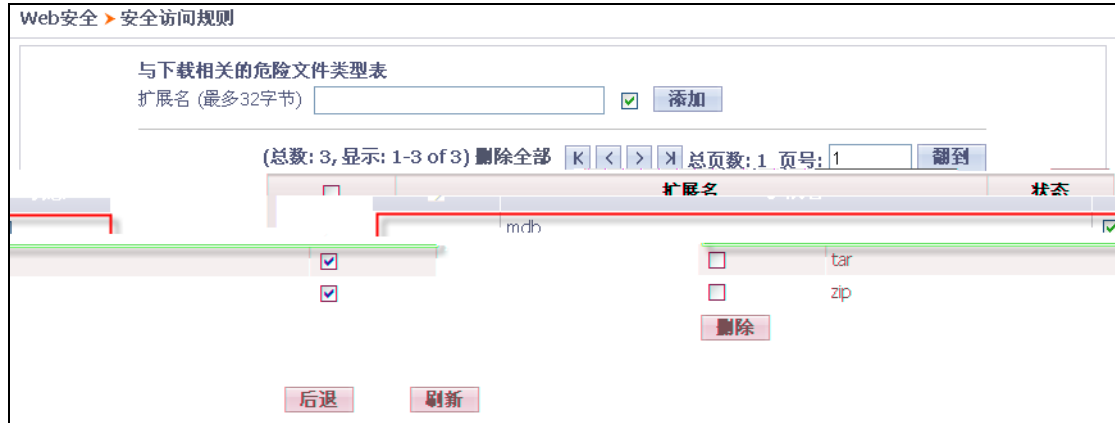
"	WEB	"	RG-WG	WEB
"	"	"	"	"
"	"	"	"	"
"	"	"	"	"

5.1.8

RG-WG	WEB
-------	-----



1	"	"	RG-WG	"
"	"	WEB	"	"
"	"	"	"	"
"	"	"	"	"
2	"	"	"	"



" mdb"

WEB

RG



Web安全 > URL安全策略

配置溢出检查

URL最大长度 (0-65536) 字节

URL参数个数 (0-1000)

URL参数内容最大长度 (0-65536) 字节

POST表单个数 (0-1000)

POST表单内容最大长度 (0-1048576) 字节

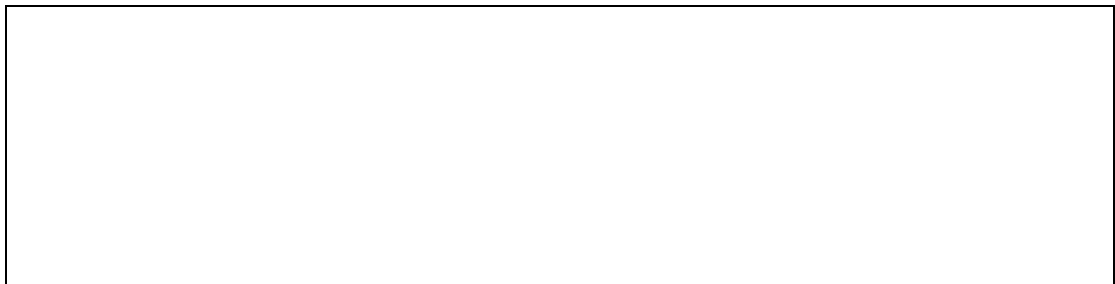
URL	URL () protocol :// hostname[:port] / path / [;parameters] [?query] #fragment URL " //" http://www.sina.com.cn/ URL 16	2048
URL	URL ? & = URL http://www.google.cn/search?hl=zh-CN&source=hp&q=Ruijie &btnG=Google+%E6%90%9C%E7%B4%A2&aq=f&oq= URL 5 & 6 URL	100
URL	URL URL / (?) name=value URL (&) URL = &	1024
POST	POST 1-1000	100
POST	POST 65536 0-1048576	post



" " WEB RG-WG
 " " " "
 " " " "
 " " " "

2

" "



A

" " " "
 " URL" " URL " " POST " " Cookie"
 " "

禁用词列表

关键词 (最多32字节)

应用域 URL URL参数 Cookie POST表单

(总数: 2, 显示: 1-2 of 2) 总页数: 1 页号: 1

<input type="checkbox"/>	关键词	URL <input checked="" type="checkbox"/>	URL参数 <input type="checkbox"/>	Cookie <input type="checkbox"/>	POST表单 <input type="checkbox"/>
<input type="checkbox"/>	法轮功	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	凶杀	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

B

" "

C



" "





3

4

Web安全 > 服务器安全组

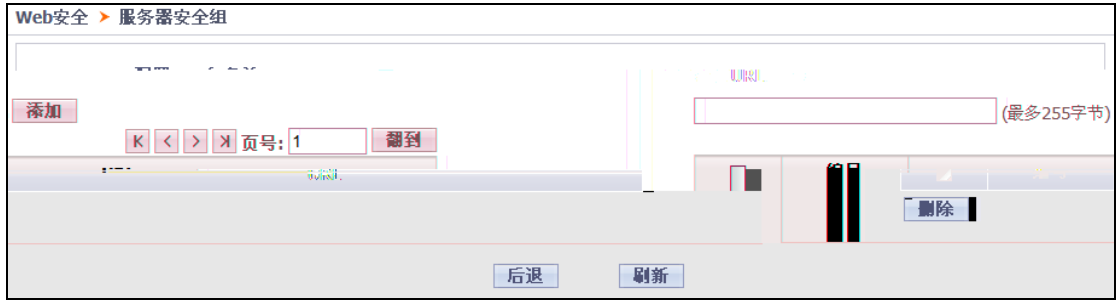
服务器安全组和安全策略
(总数: 42, 显示: 1-25 of 42) 删除全部

总页数: 2 页号: 1 翻到

编号	名称	状态	移动
1	default-g	启用	1
2	1	启用	1
3	123	启用	1,2,3
4	2	启用	2
5	3	启用	3
6	4	启用	4
7	6	启用	6
8	7	启用	7
9	8	启用	8
10	9	启用	9
11	10	启用	10
12	11	启用	11
13	12	启用	12
14	13	启用	13
15	14	启用	14
16	5	启用	5
17	15	启用	15
18	16	启用	16
19	18	启用	18
20	19	启用	19
21	17	启用	17
22	20	启用	20
23	21	启用	21
24	22	启用	22
25	23	启用	23

添加 编辑 删除

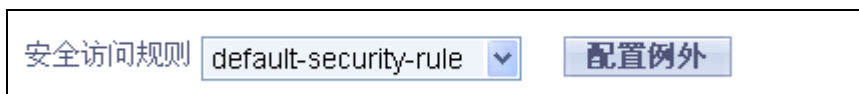




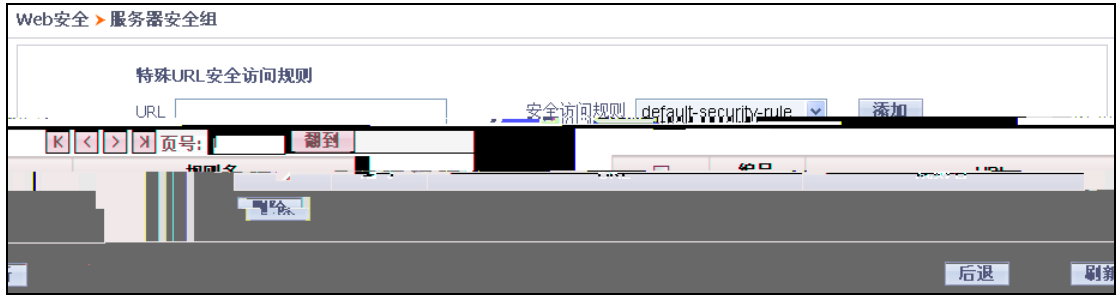
“ URL ” WEB URL
 path level URL “ ”
 URL
 www.sina.com URL

5.2.4 URL

URL URL Web
 URL URL URL
 URL URL
 5.1URL
 1 WEB URL

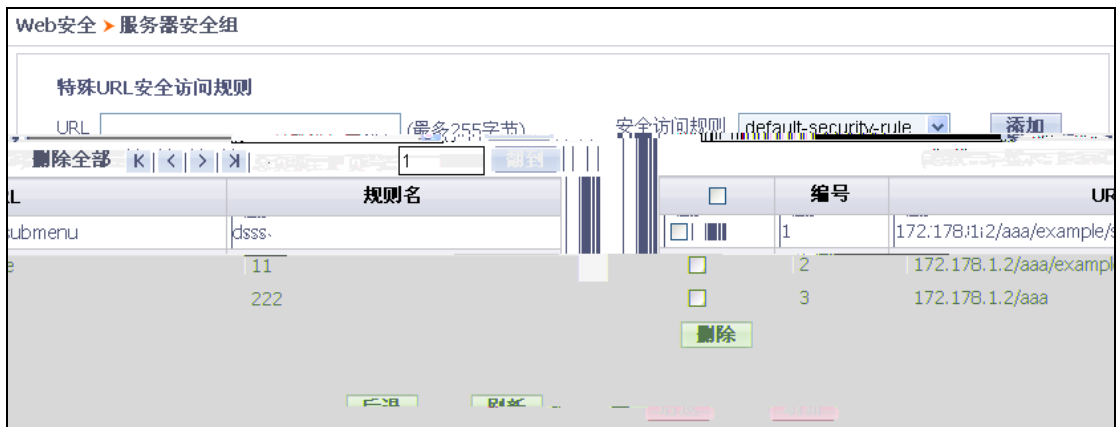


2
 “ URL ”
 “ URL ”



A

" URL" URL " URL"
" URL" " " "



B

" "

5.2.5

RG-WG

WEB

FTP

1

HTTP

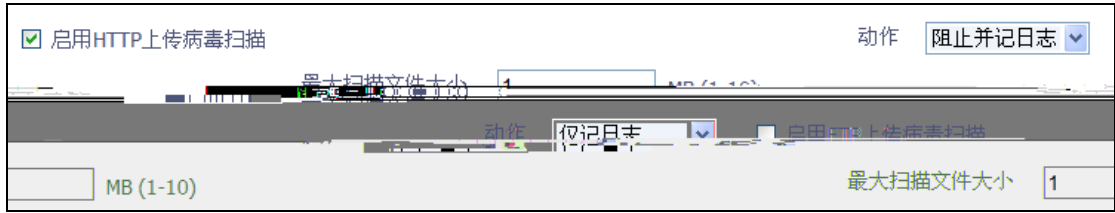
" "

FTP

" "

RG-WG

" "



1	WEB
2	WEB
3	WEB
2	
	1M

5.2.6 Cookie

RG-WG	WEB	Cookie	
	IP	Cookie	Cookie
1	"	" "	Cookie "



	WEB	Cookie	
	IP	Cookie	Cookie
	Cookie	"	" "
Cookie	" "	Cookie	IP" "
	RG-WG		



SQL

Cookie

Cookie RG-WG

Cookie

Cookie

1 W



RG-WG	URL
<script src=" http://domain/....." >, domain WEB	<iframe src=" http://domain/....." > domain RG-WG
" "	HTTP
1	WEB
2	WEB
3	WEB

UDP Flood

ICMP Flood

Dos

RG-WG

Dos

1 Web

5.5 WEB

RG-WG

WEB

GB

1-50

2 " "

5.5.2

5.5.1

1 Web > Web >

Web安全 > Web缓存 > 实时监控

URL: 端口:

缓存内容:

启用编码自动转换
(总数: 8, 显示: 1-8 of 8)

总页数: 1 页号: 1

URL	端口	缓存文件时间	服务器文件时间	缓存文件	服务器文件	开始监控时间
443	2009-03-18 02:40:41	2009-03-18 02:40:41	2010-06-29 08:26:35	172.17.1.130/ftp/automaile...		
...
...	80	2009-03-18 02:13:13	2009-03-18 02:13:13	2010-06-29 08:35:25	172.17.1.130/ftp/automaile...	
...	80	2009-08-26 14:41:48	2009-08-26 14:41:48	2010-06-29 09:02:00	static.googleadserving.c...	
...	80	2010-05-30 22:21:11	2010-05-30 22:21:11	2010-06-29 08:46:15	update.360safe.com/v3/...	
...	80	2010-06-28 20:35:01	2010-06-28 20:35:01	2010-06-29 08:49:15	update.360safe.com/v3/...	

>

2

" URL "

5.6

WEB	HTTPS	HTTPS
	certificate	
		Web
RG_WG	WEB	
	WEB	
	RG_WG	WEB
		Web
	WEB	
	Web	

5.6.1

RG_WG	WEB	PEM
PFX		
1	Web	> >



2

A " "

B PEM PFX

C

PEM

PFX

D " "

3

" "

5.6.2

WEB



2

" " IP " IP

3

" "

4

" " " "

6.2

Ruijie RG-WG IP WEB

SQL

" block" RG-WG IP
WEB

IP

IP

WEB

1

/ >

黑名单/白名单 > 动态攻击黑名单

启用动态攻击黑名单
锁定时间: (1-7200) 分钟
 在攻击日志中记录事件

动态攻击黑名单

下面的IP将不会被加入动态攻击黑名单

客户 IP/子网掩码:

页号:

<input type="checkbox"/>	源IP/子网掩码
<input type="checkbox"/>	

2

"

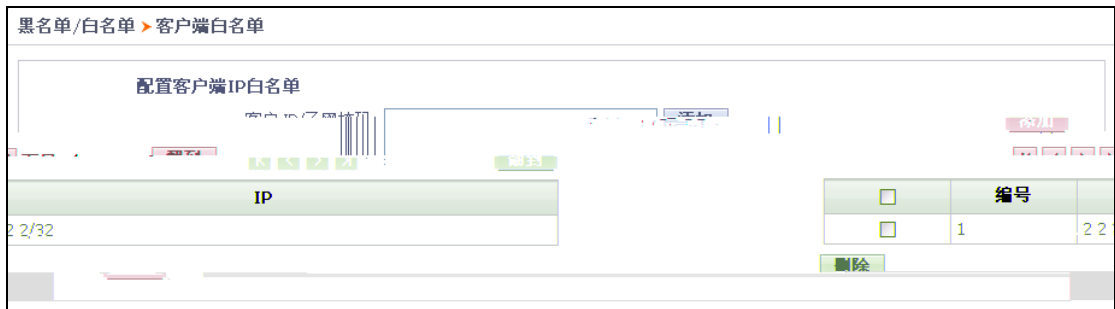
"

R

6.3

2 WEB IP

1 / >



2

" IP "

7

7.1

7.1.1

1

>

>



管理 > 系统设置 > 语言

语言: 简体中文

应用 取消

2 " "

3 " "

7.1.2

管理 > 系统设置 > 主机

主机名

当前主机名 **RG_WG**

新主机名

启用SNMP

只读共同体

系统时钟

手动设置日期/时间为:

年 月 日

时 分 秒

时区偏移

启用NTP服务

服务器名称

自动同步时间间隔 (12-180 分钟)

... DNS " " 202.106.0.20

备选DNS服务器

7.1.2.1

" "

" "

' _

" "

7.1.2.2 SNMP

- 3 SNMP SNMP
- a > >
- b SNMP
- c " " " SNMP"
- d " "

7.1.2.3

1

“ ”

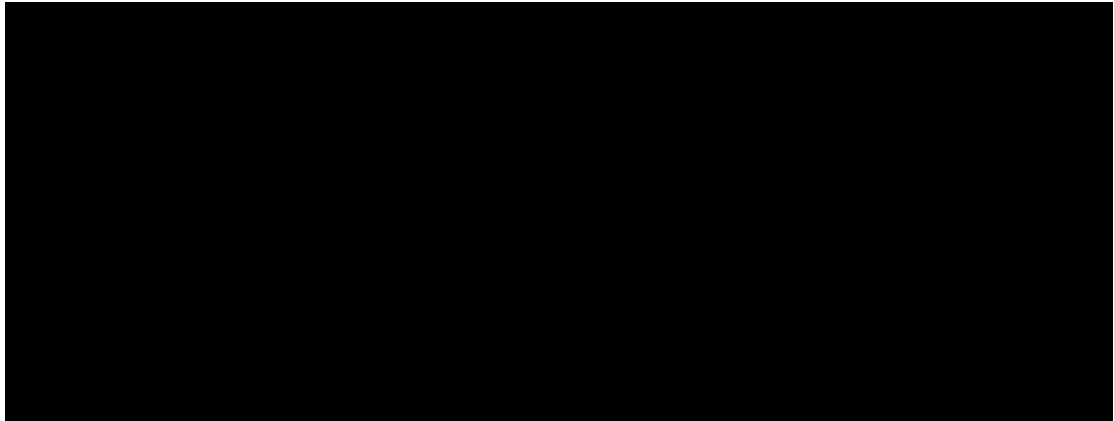
2

7.1.3.1

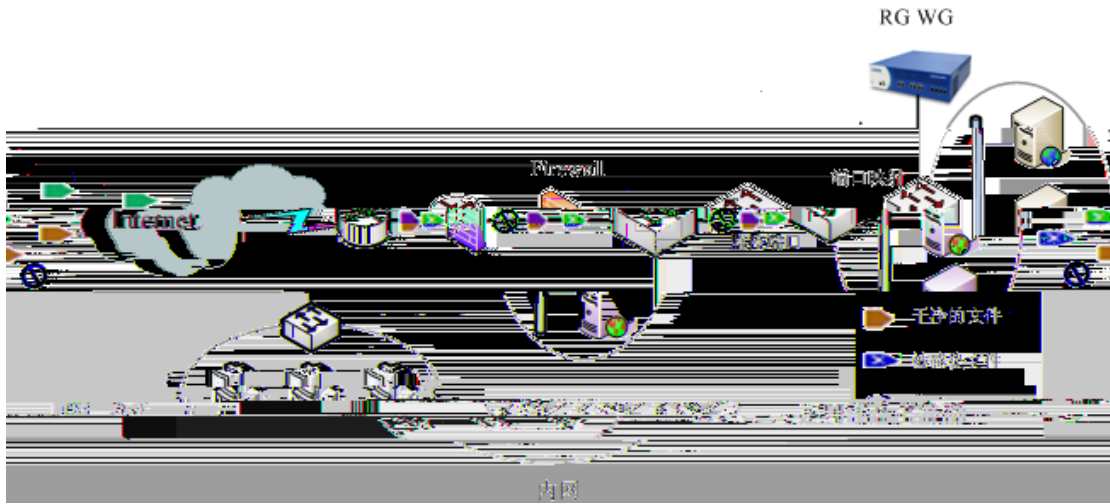
HTTP/HTTPS
WEB
WEB

WEB

WEB

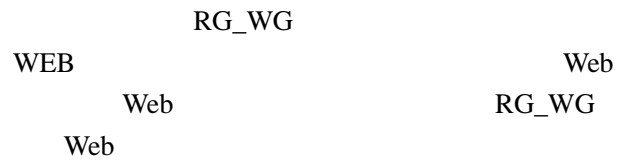


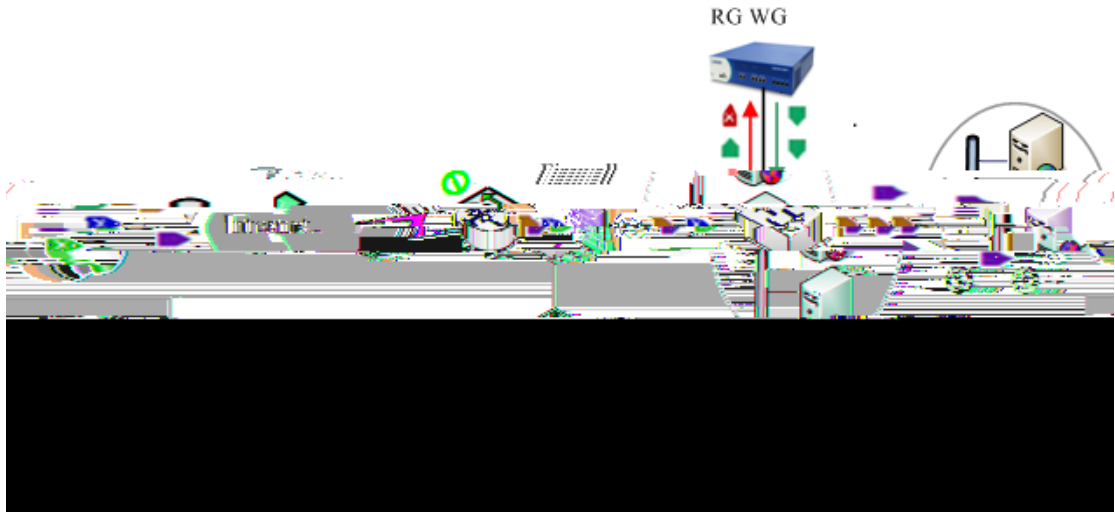
SPAN



span

- WEB
-

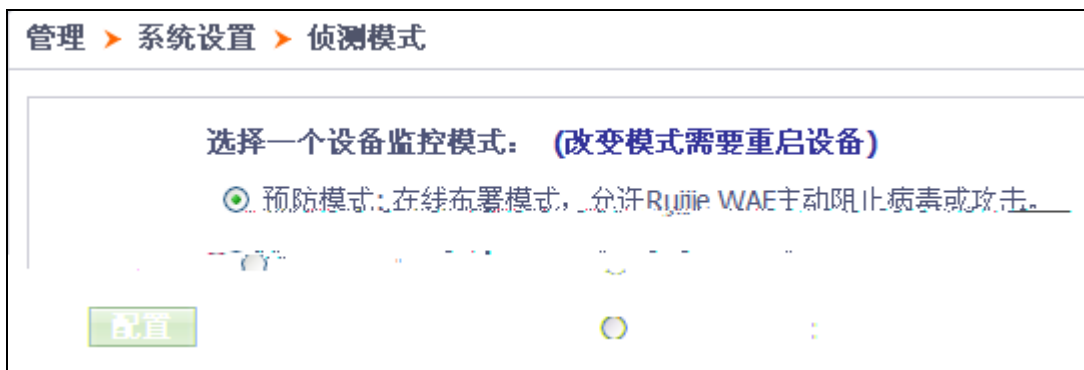




WEB

1 > >

2



" "

A > >

B > >
IP

C " " IP WEB IP

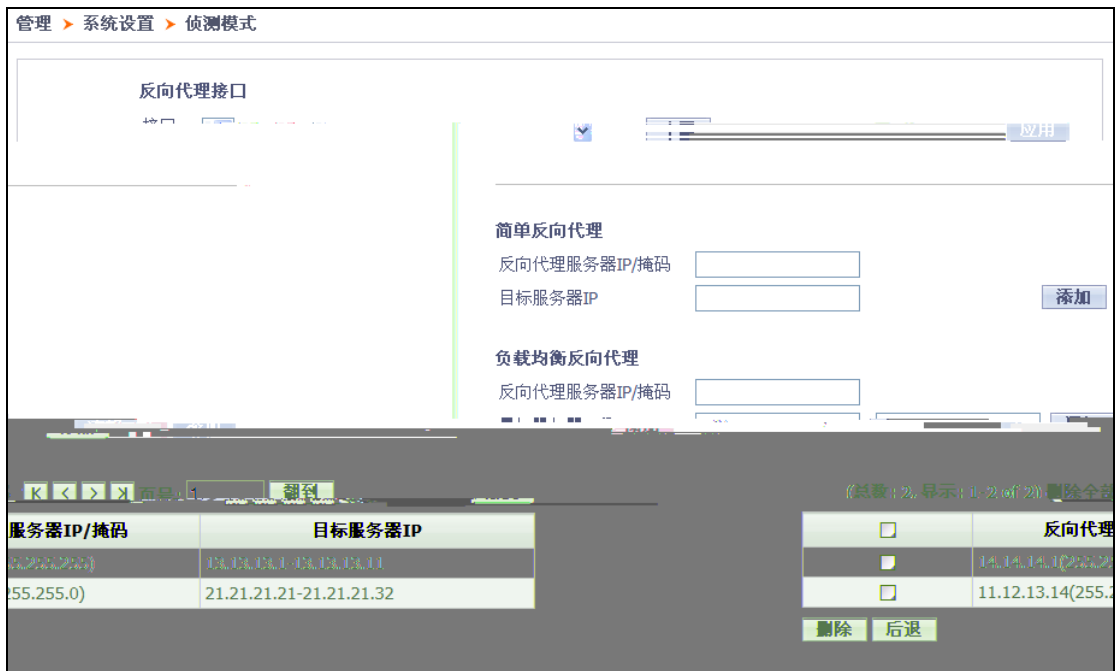
Web " " RG_WG

" IP/ " RG_WG WEB

IP

" IP" RG_WG Web IP

" IP " WEB IP



3 " "

4

7.1.3.2

RG-WG
failopen
WEB

bypass

1 > >

设置Fail-safe工作模式:

当网络流量超出系统处理能力时, Fail-safe模式会用来处理匹配到内容过滤策略的新建连接,而对于匹配到通过策略或者通过FQDN接口的其他流量则不生效。

- Fail-open: 策略匹配到内容过滤策略的新建连接。
- Fail-close: 策略匹配到内容过滤策略的新建连接。

2

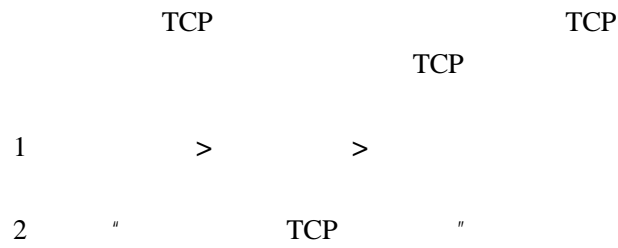
Fail-open

WEB

Fail-close

7.1.3.4

TCP



启用严格的TCP连接检查

启用严格的TCP连接检查将允许系统对每个TCP连接进行严格检查,丢弃那些没有完成三次握手过程
的TCP连接,有效防止恶意攻击。

3 " "

7.1.4

HA
QMAIL

WEB

管理 > 系统设置 > 警告通知 > 邮件配置

发送邮件地址

接收邮件地址

邮件转发服务器设置:

转发服务器地址或名称

服务器要求安全传输 (SSL)

端口 (0-65535)

SMTP 认证

SMTP 用户名

密码

使用邮件转发服务器 告警邮件 报表邮件 隔离邮件

2



1 > >

管理 > 系统设置 > 日志 > 系统日志设置

日志磁盘管理

最大保存天数 (30-365)

最大磁盘空间 (5000-50000) MB

最大使用率 %

启用系统日志

攻击事件

病毒事件

访问事件

管理事件

系统事件

导出日志

为避免日志丢失，定制日志计划将日志定时导出到外部服务器。本操作将导出所有类别的日志。

导出定时设置 按星期 按天数

每隔 天 (1-30)

导出时间 (hh:mm)

导出日志到FTP服务器

服务器IP

用户

密码

2

	5000-50000 MB

1

	4 4.2.4
	5 4.2.5
	HA

3 FTP

" "

--	--

	/
	()

Syslog sy

HA

WEB

WEB

Syslog

3

Syslog

IP

Syslog

IP

Syslog

Syslog

" Syslog "

" " " "

syslog

7

0

7

4

"

"

7.1.7

RG-WG

SNMP Trap

HA

"

"

7.1.4

7.1.7.1

RG-WG

HA

HA

"

"

WEB

1

>

>

>



2

a

b

10

1-1440
1-10000

c

"

"

6 HA

HA

"

HA

"

7

"

"

"

"

8

"

"

7.1.7.2 SNMP Traps

SNMP trap

SNMP

SNMP

SNMP v1 v2

SNMP

7.1.2.2 SNMP

SNMP

SNMP trap

SNMP

1

>

>

> SNMP Traps

管理 > 系统设置 > SNMP Traps

Trap版本:

SNMP服务器 1# IP: 共同体: 端口:

SNMP服务器 2# IP: 共同体: 端口:

SNMP服务器 3# IP: 共同体: 端口:

2

Trap

SNMP

SNMP

SNMP

Trap

SNMP

Trap

3

" "

7.2

7.2.1

4 88

RG-WG

2

IP TCP

IP

RG-WG

WEB

ASIC

WEB

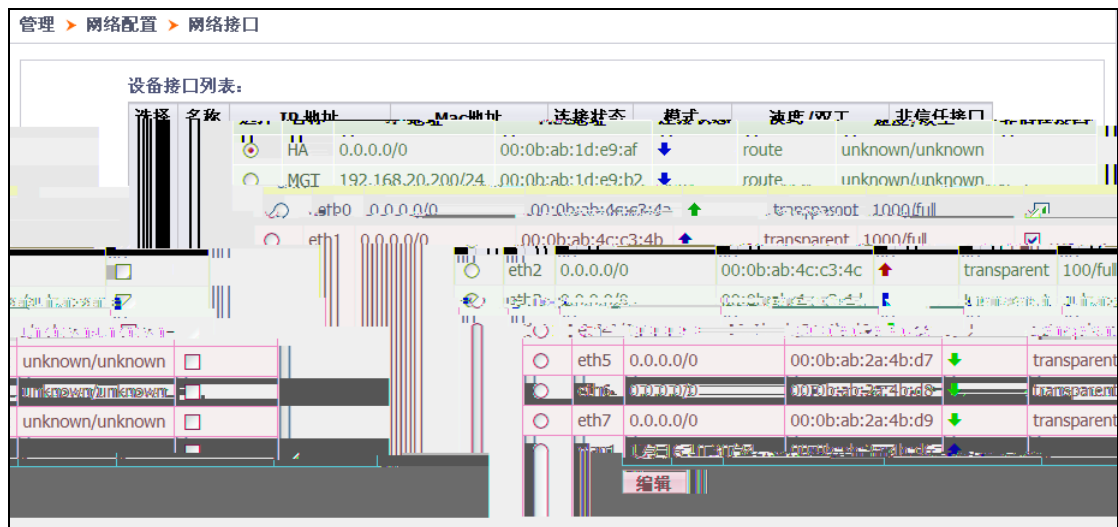
WEB

7.2.1.2

1

>

>



VLAN

HA

HA

RG-WG2000

RG-WG3000

RG-WG1000

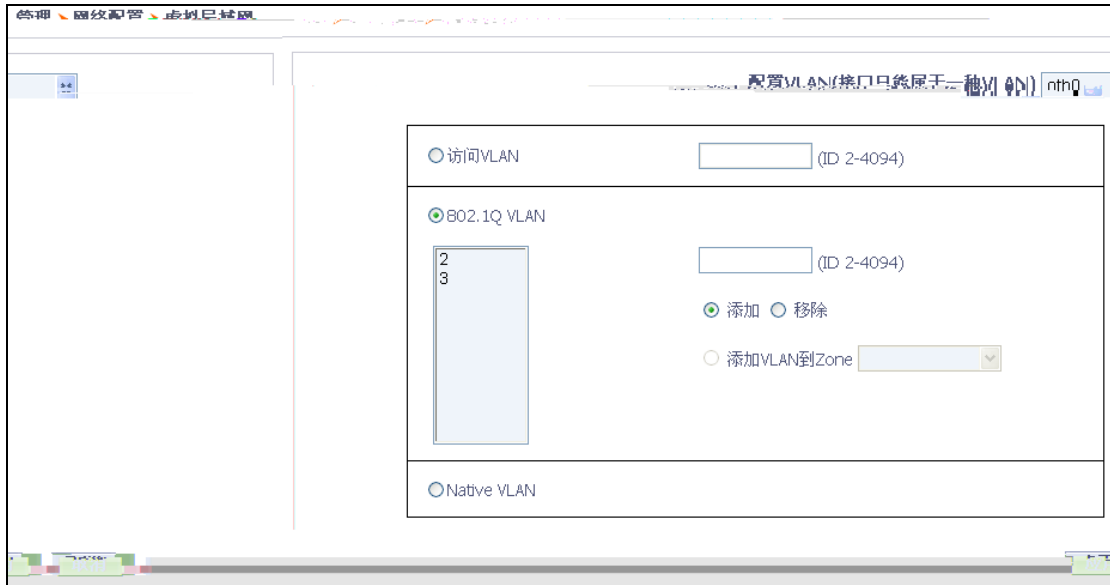
RG-WG1000S

MGT



IP /	IP
	" " " "
	HTTPS SSH PING SNMP
" Up"	/ " D

1 > >



2

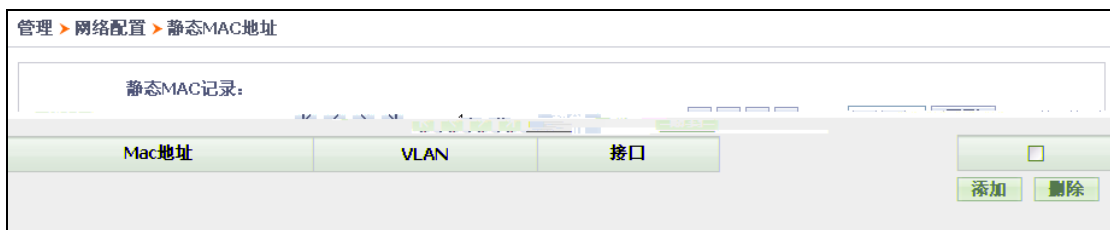
	Access	Trunk			
Access	"	VLAN"			
VLAN ID					
Trunk	"	802.1Q VLAN"			
VLAN ID					
	ID	"	"	"	"
	VLAN ID		VLAN ID		
		VLAN ID	"	"	"
		VLAN ID		VLAN ID	
	Trunk	Native VLAN	VLAN1		

" Native VLAN" VLAN 1 VLAN 1
" " "

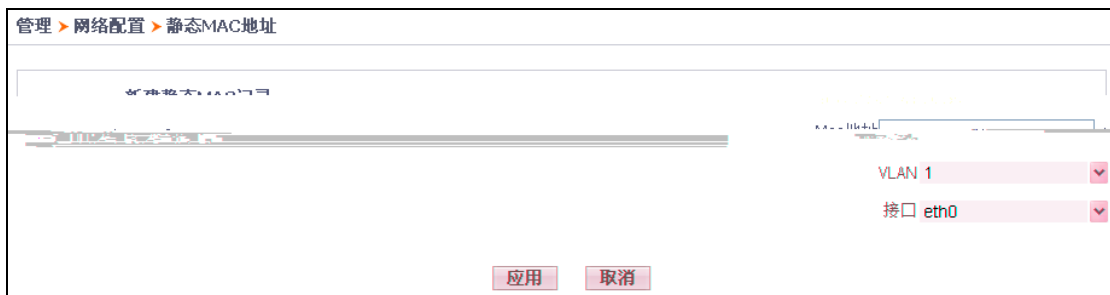
7.2.3 MAC

MAC
MAC

1 > > MAC



2



" "

ARP

" "

7.2.5

VLAN

IP

B " "

" "

7.2.6

RG-WG Virtual Router Redundancy
Protocol VRRP

7.2.6.1

RG-WG

RG-WG VRRP

HA

VRRP

RG-WG

1 3

VRRP

2

Down

VRRP

3

ping

VRRP

4 RG-WG

5 " "

7.2.6.2 HA

HA

1

2

HA

eth4

HA

eth4

HA

2 " HA "

" HA " " Master "

" backup "

" MAC Block " HA MAC
VRRP

3 ID IP

A " IP / " IP

IP

HA

B " HA "

HA

254 1-254

C " ID

B " IP " IP
HA IP
C " "

A " "

B " " HA €
w ÄQ 1-32 È

VRRP

2 " "

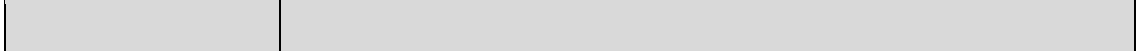
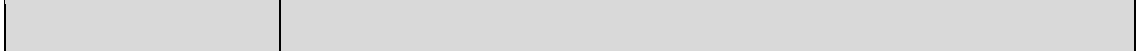
:

IP

7.3.1.2

WEB

1 > > > ~~10.1.1.1~~



WEB

a > > >
b " " " " " " WEB
" " " " " "
5

a > > >
b " " " " " " WEB
" " " " " "
6

回滚到先前病毒特征库 回滚到先前的Web攻击特征库

" " " " WEB
" " " " " "
" " " " " "
Web " "

1 > > >

管理 > 系统维护 > 系统更新 > 代理认证

代理认证

启用代理认证

到认证服务器

认证服务器IP地址

端口 (1-65535)

用户名

密码

系统 will 发送以下的证书

域 (只用于NTLM认证)

认证服务器IP地址

端口

用户名

密码

应用 取消

	<p>1 None-auth IP</p> <p>2 Basic / IP</p> <p>3 NTLM Windows AD</p>
	<p>NTLM</p> <p>Windows</p>
IP	IP

2 " "

7.3.2

RG-WG WEB
WEB

" "

License

WG License License License

License

1 > >



2

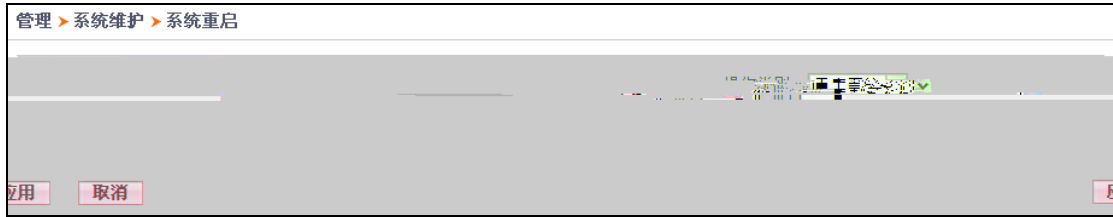
" "

" "

7.3.3

WEBUI RG-WG

1 > >



2 " "

3 " "

7.3.4

" "

FTP

1 > >



2 " "

3

PC

7.4

RG-WG

administrator
CLI

administrator

WEB

7.4.1

RG-WG

WEBUI CLI

" "

管理 > 访问管理 > 用户账号

管理员名称

新密码

有效密码格式:

- 长度必须在6到20之间
- 数字和特殊字符
- 字母和特殊字符
- 数字和大、小写字母
- 字母、数字和特殊字符

确认新密码

应用 重置

	" "
	Read-write ---
	Read-only ---
	Audit --

3 " "

7.4.2

HTTPS SSH

1 > >

管理 > 访问管理 > 访问控制

空闲超时值 (5-30)分钟

登录重试次数 (0-10)次

锁定时间 (5-30)分钟

HTTPS端口

SSH端口

管理主机

		WEBUI	
	5-30	15	
	0-10	5	
	"	"	
	5-30	5	
HTTPS	HTTPS		443
SSH	SSH		

" "

3

" "

4

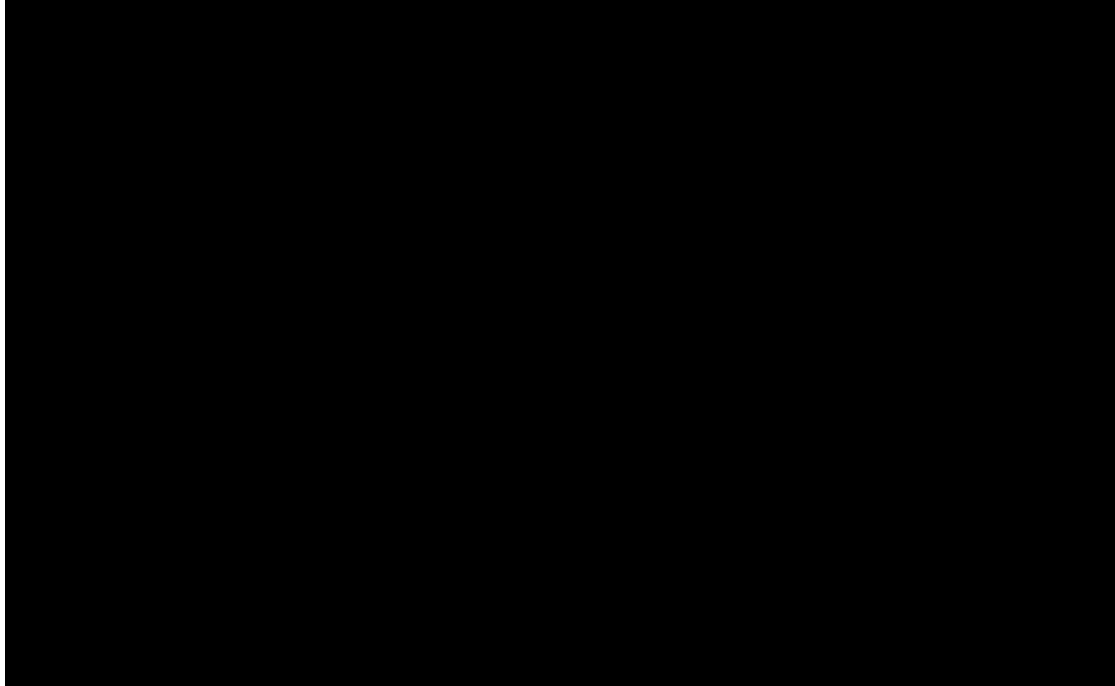
" "

3

" "

A

RG_WG
RG_WG



1 RG_WG

2

" "

" "

3 WEB



Malware_Alert

HTTP

IP WEB IP

IP WEB IP

URL URL

block_log

sp_attack: Client_IP=<ip_address> Server_IP=<ip_address> URL=<URL>
Attack=<SQL Injection | Command Injection | XSS | Overflow| Embed Trojan|
URL Blacklist | Overflow | Unauthorized IP| Customized SQL Injection |
Customized XSS | Customized Command Injection | Forbidden Word | Weak
Password | Dangerous Upload | Dangerous Download | Infected Site | Database
Error | Directory Explore | Source Code Leak | Client IP Blacklist | Attacker IP
Blacklist | Response Error | Unauthorized Cookie > Action=<Blocked |
block_log > Method=<GET|POST>

WEB

sp_access

IP WEB IP

IP WEB IP

WEB GET

URL POST

URL URL

WEB

sp_access:src_IP=<ip_address> dst_IP=<ip_address> URL=<URL>
Method=<GET|POST> ReturnCode=<number>

IP

IP

