

---

RG-WG

WebGuard

---

# **1**

## **1.1**

---

Ruijie RG-WG HTTP/HTTPS

WEB

Cookie

Ruijie RG-WG

WEB

Cookie

IP

Cookie

Cookie

Ruijie RG-WG

HTTP/HTTPS

---

## 1.3

[www.ruijie.com.cn](http://www.ruijie.com.cn)

" "

4008111000.

## 2

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

### 2.1

	HTTPS	WEB	WG
Internet Explorer 6.0	6.0		
Firefox 1.5.0	1.5.0		
PC	WEBUI	IP	192.168.20.100/24
	WG eth0	WEBUI	
1	WEB		
https://<Ruijie_gateway_ip_address>			

---

2 WEBUI WEBUI  
CLI IP

**1**

IP 192.168.20.200  
administrator  
password  
English

3 WEBUI

4 " "

" "

---

## 2.2

WEBUI



---

WEBUI

密码长度	<input type="text" value="8"/>	(5-30)分钟
登录失败次数	<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

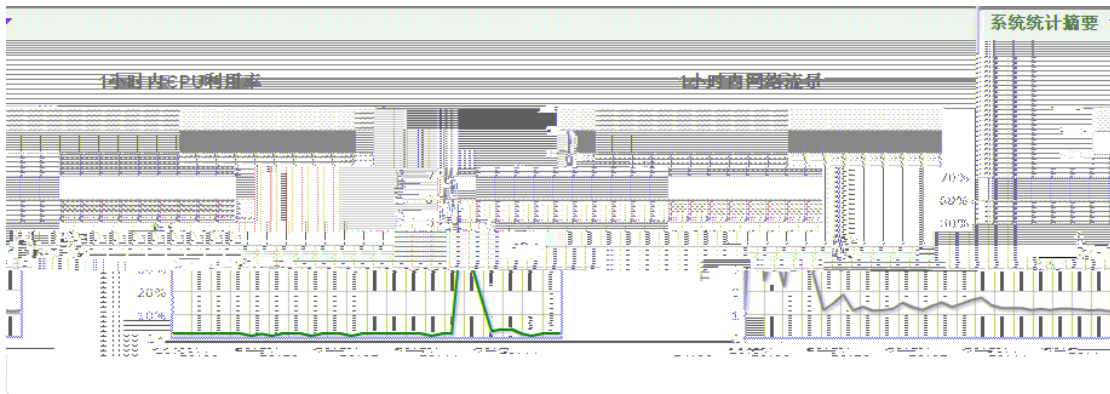
1



7.1.2.1

	" " " "
	7.1.3.1
HA	HA " " " " " "
	HA 7.2.6
	" " " " 7.3.1.1
	" " 7.3.1.2
	" "
WEB	7.3.1.2
WEB	

2 " " CPU



" "

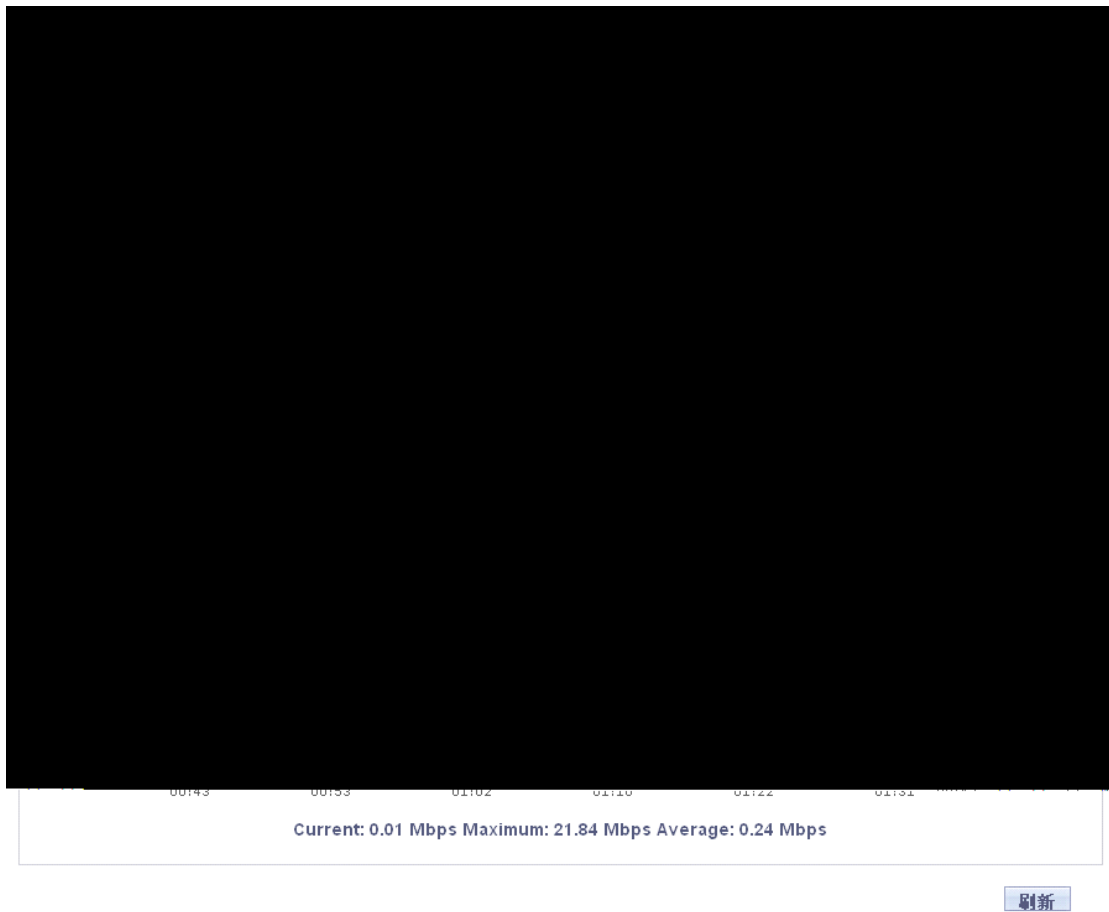
---

## 3.2

RG-WG

### 3.2.1

CPU



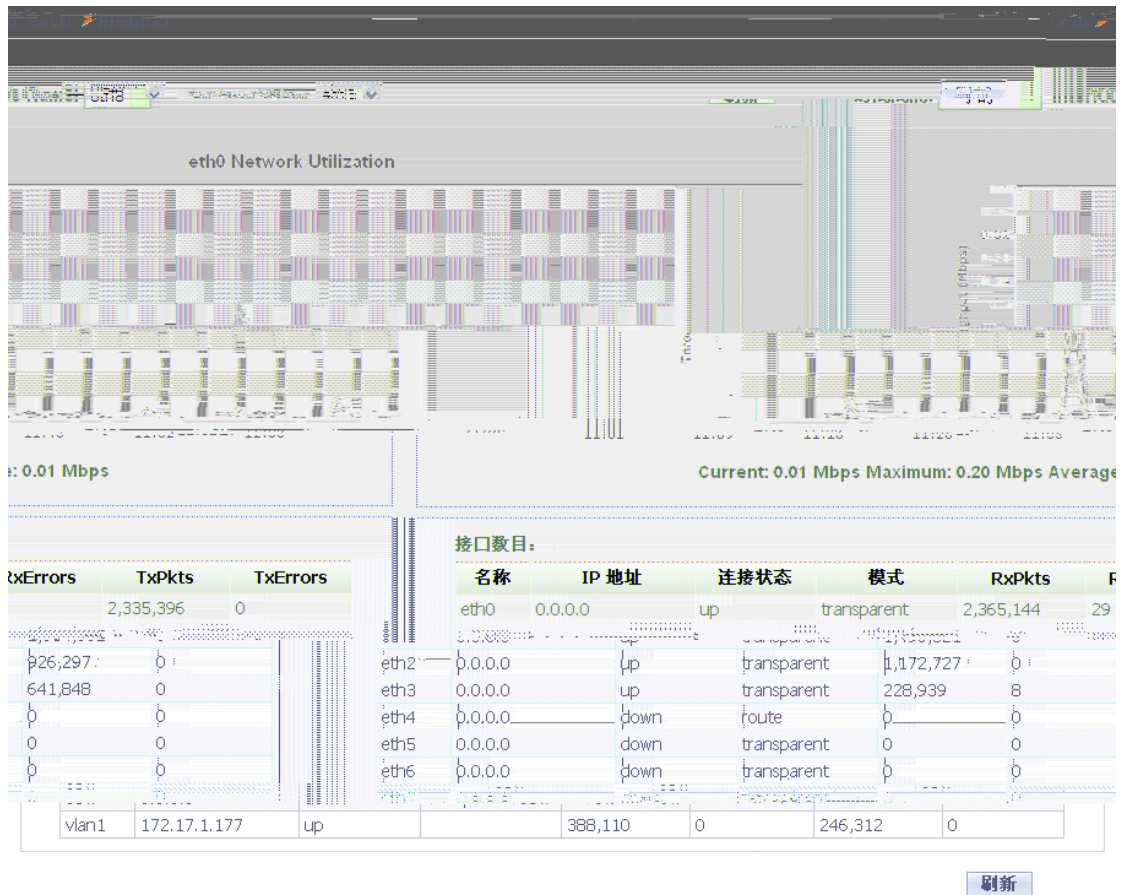
" CPU "

CPU

CPU

“ ”  
 “ ”  
 “ ”

### 3.2.2



IP	0.0.0.0
	“ up” “ down”
	vlan1      vlan1

	vlan1 vlan1
	" " " "
Rx Pkts	
Rx Errors	
Tx Pkts	
Tx Errors	

" "

" " " "

### 3.2.3

WEB

WEB

WEB

WEB



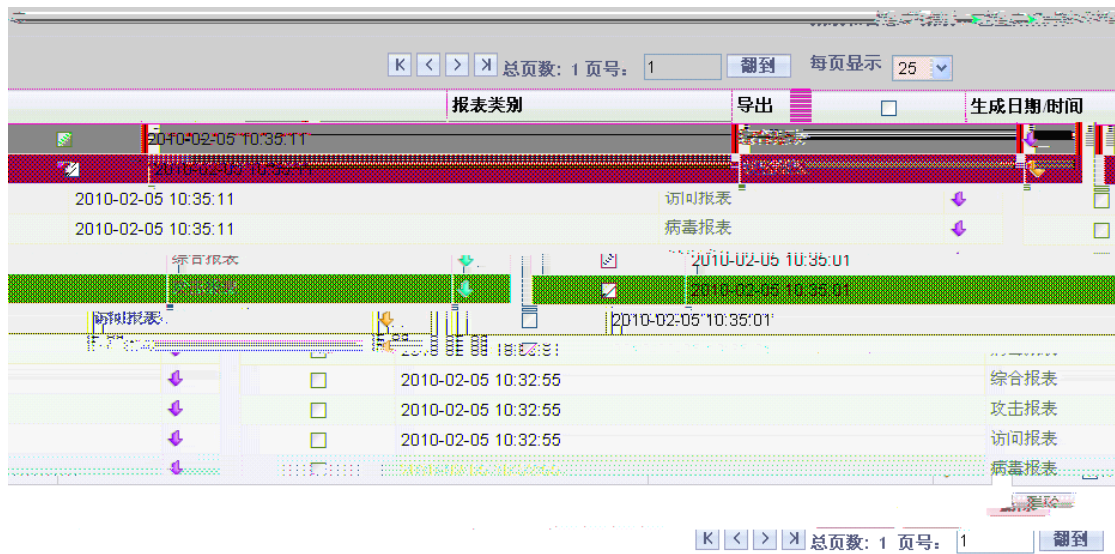
WEB	WEB
WEB	10 WEB
IP	10
IP	10 WEB
" "	" "
" "	" "



## 4.1.1

" "

1



2

" "

3

" "

PC

4

" "

## 4.1.2

7.1.4

1

---

---

“ ”  
WEB WEB  
“ IP / ” IP  
WEB

4

“ ”  
A “ ” “ ”  
B “ ”

5

“ ”  
A “ ”  
B “ ”  
7.1.4  
“ ”  
“ ”

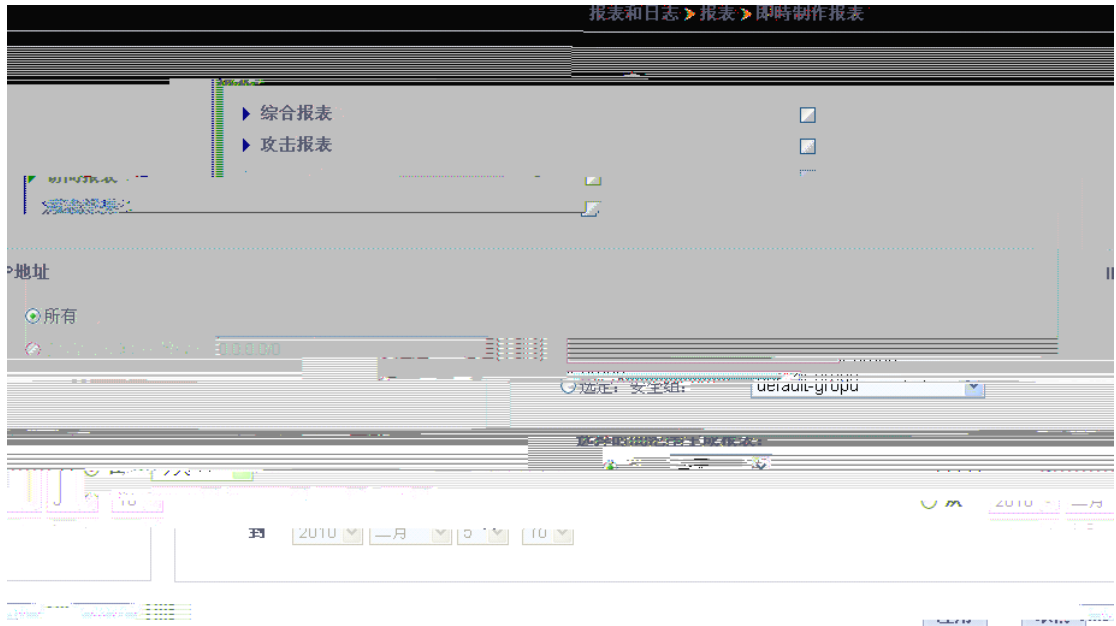
English

6 “ ”

### 4.1.3

WEBUI

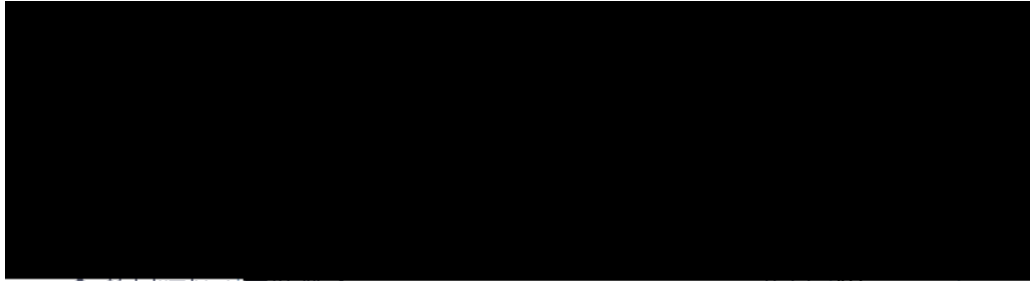
1



2 " " " " " "

" " " " ▶ "

" "



● 各客户端攻击事件排名 数目 10

ÀBÿ ÿ <'X4³Añ ÌB²

---

A " " "

---

## 4.2.1

SQL

WEB

WEB

IP WEB

WEB

URL

URL

POST

Cookie

WEB

IP

WEB

Cookie

http

1



URL

URL

3

"

"

4

PC

"

"

HTML

CSV

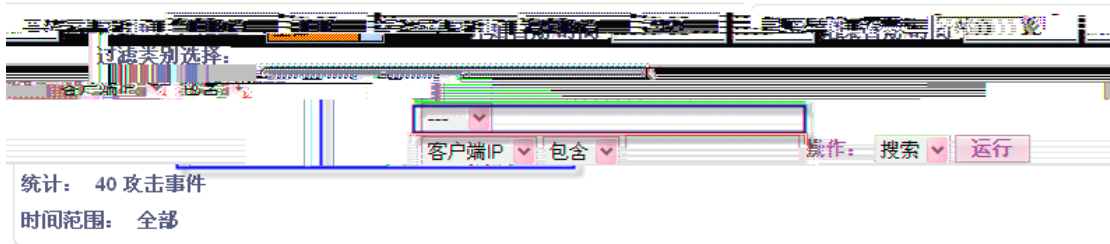
"

"

5

IP

IP



A

"

/

"

"

"

00:00:00

"

"

00:00:00

"

7

"

"

"

1 00:00:00

"

30

"

30

"

"

"

/

"

"

/

"

B

"

"

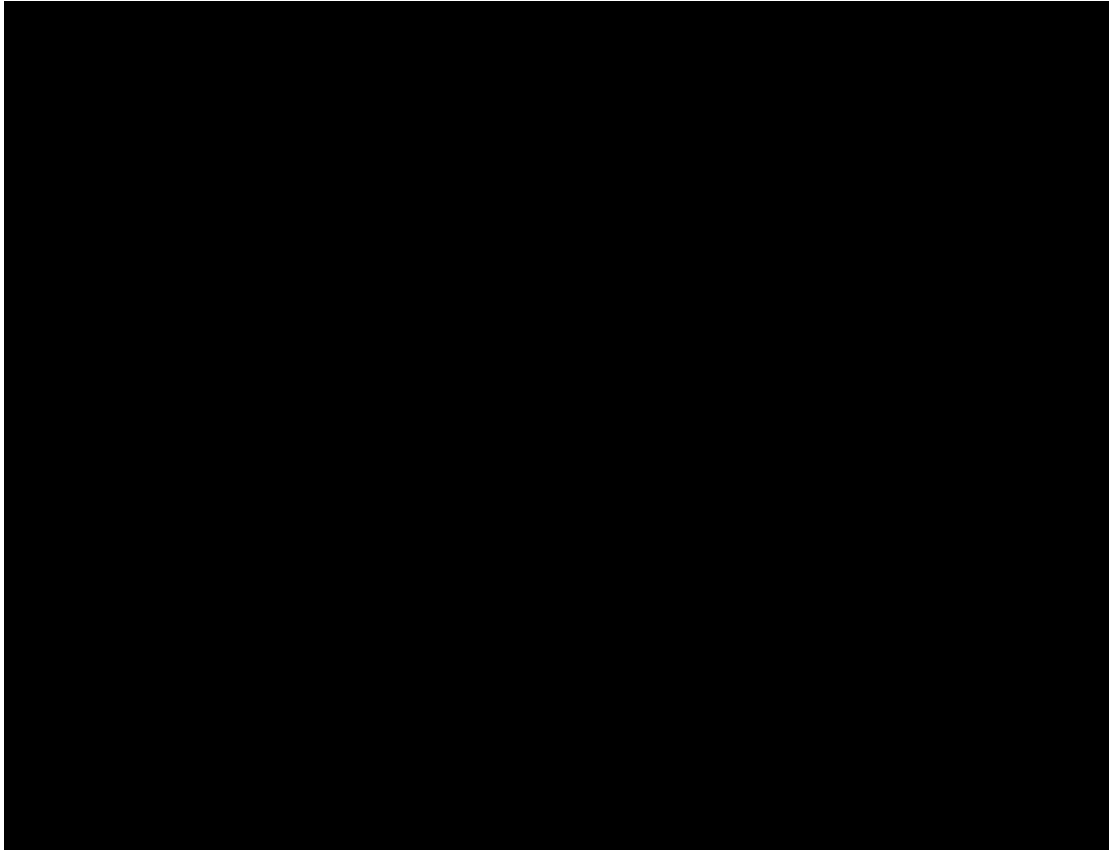
"

"

"

"

---



"

"

"

"

25

"

"

"

"

"

"

2



IP

WEB

IP

IP

WEB

IP

URL

URL

---

33 3

)

---

" "

" "

C " "

" "



Source IP	Destination IP	Method	Protocol	Source Port	Destination Port	Status	Time
172.17.1.126	123.129.242.170	POST	http	80	80	200	2010-02-05 12:14:20
172.17.1.126	123.129.242.170	POST	http	80	80	200	2010-02-05 12:09:20
172.17.1.126	65.197.197.50	GET	http	80	80	200	2010-02-05 12:06:13

" " " " " "

2

	WEB	
IP	WEB	IP
IP	WEB	IP
	WEB	GET

---

3

3

3

---

“ ”

“ ”

C “ ”

“ ”

“ ”

D “ ”

“ ”

“ ”



## 4.2.4

1

报表和日志 > 日志 > 管理 > 管理员日志

结束日期时间: 20090101 2359 日期时间范围: 全部 开始日期时间: 20000101 0000  
过滤类别选择:

搜索 运行 统计: 372 管理事件 时间范围: 全部

操作	日期 时间	来源IP	管理员	动作
ebUI port 443	2009-12-31 13:19:26	192.168.11.131	administrator	administrator logged in from the W
d successfully from webUI	2009-12-31 11:29:35	192.168.11.131	administrator	manually update Firmware: update
	2009-12-31 11:29:09	192.168.11.131	administrator	exec update firmware
	2009-12-31 11:14:55	192.168.11.131	administrator	set dynamic-blacklist
max-url-length 1	2009-12-31 11:09:40	192.168.11.131	administrator	server group yzf: set anti-overflow
	2009-12-31 11:08:23	192.168.11.131	administrator	set anti-overflow max-post-data-length 134
istrator Unset client-blacklist entry 172.17.1.125/32	2009-12-31 11:08:21	192.168.11.131	admini	
nistrator unset client-blacklist entry 172.17.1.125/32	2009-12-31 11:08:05	192.168.11.131	admini	
	2009-12-31 11:07:10	192.168.11.131	admini	
istrator set interface eth1 inbound	2009-12-31 11:07:07	192.168.11.131	admin	
istrator set client-blacklist entry 172.17.1.125/32	2009-12-31 11:04:46	192.168.11.131	admin	
istrator set dynamic-blacklist entries 72.37.33.9/32	2009-12-31 11:03:36	192.168.11.131	admin	
max-post-data-length: 2048	2009-12-31 10:54:06	192.168.11.131	administrator	server group yzf: set anti-overflow ma
	2009-12-31 10:49:09	192.168.11.131	administrator	server group yzf: set anti-overflow max-post-data-length 134
10:45:46	2009-12-31 10:45:46	192.168.11.131	administrator	server group yzf: set anti-overflow max-post-form-fields 9
10:44:44	2009-12-31 10:44:44	192.168.11.131	administrator	server group yzf: set anti-overflow max-post-form-fields 7
max-post-form-fields 7	2009-12-31 10:43:54	192.168.11.131	administrator	server group yzf: set anti-overflow ma
	2009-12-31 10:40:53	192.168.11.131	administrator	server group yzf: set anti-overflow max-post-form-fields 1
	2009-12-31 10:34:16	192.168.11.131	administrator	server group yzf: set anti-overflow max-post-form-fields 7
	2009-12-31 10:22:51	192.168.11.131	administrator	server group yzf: unset trojan-detection

总页数: 15 页号: 1

" "

" "

" "

" "

"

2

IP	IP

3 " "

4 PC " "

HTML CSV " "

5

IP IP

开始日期/时间 19000101 0000 结束日期/时间 20990101 2359 日期/时间 范围: 全部

过滤类别选择:

包含 管理员

管理员 包含 操作: 搜索 运行

统计: 372 管理事件  
 时间范围: 全部

A " / "

" " 00:00:00

" " 00:00:00

" 7 "

" " 1 00:00:00

" 30 " 30

" " " / " " / "

**1**

B " "

" " "

"

---

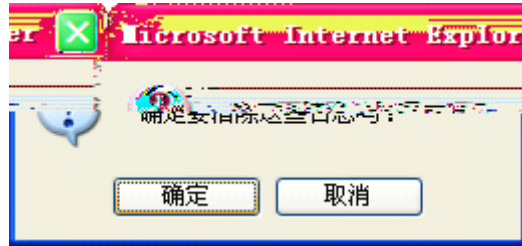
C " "

" "

D " "

" "

" "



## 4.2.

HA

1

90101 2358 日期/时间/范围: 全部 开始日期/时间: 19000101 0000 结束日期/时间: 200912312358  
 过滤类别选择: 系统事件 包含 系统事件 包含 操作: 搜索 运行  
 时间范围: 全部  
 每页显示: 25 启用编码自动转换  
 总页数: 26 页号: 1 清除所有日志 导出文件类型: HTML 导出日志  
 日期 时间 系统事件  
 sec 2009-12-31 13:24:02 Adjust time from NTP server 72.18.205.156 offset 0.044053  
 sec 2009-12-31 13:12:02 Adjust time from NTP server 72.14.179.211 offset 0.024885  
 c 2009-12-31 13:00:03 Adjust time from NTP server 38.229.71.1 offset 0.037535 se  
 \*SEC 2009-12-31 12:45:07 Adjust time from NTP server 193.50.144.194 offset 0.0357537  
 2009-12-31 12:29:00 Adjust time from NTP server 72.18.205.167 offset 0.054210 sec 2009-12-31  
 -31 12:12:07 Adjust time from NTP server 72.167.54.201 offset 0.024298 sec 2009-12-  
 -31 12:00:03 Adjust time from NTP server 216.45.57.38 offset 0.037118 sec 2009-12-  
 2009-12-31 11:34:29 interface eth3 is off 2009-12-31 11:34:29  
 2009-12-31 11:34:28 interface eth3 is on speed:1000 duplex:FULL 2009-12-31 11:34:28  
 2009-12-31 11:34:28 interface eth3 is on 2009-12-31 11:34:28  
 2009-12-31 11:34:28 interface eth3 is on speed:1000 duplex:FULL 2009-12-31 11:34:28  
 2009-12-31 11:34:23 interface eth1 is on speed:1000 duplex:FULL 2009-12-31 11:34:23  
 2009-12-31 11:34:22 interface eth2 is on speed:100 duplex:FULL 2009-12-31 11:34:22  
 2009-12-31 11:34:22 interface eth0 is on speed:100 duplex:FULL 2009-12-31 11:34:22  
 2009-12-31 11:34:21 interface eth4 is off 2009-12-31 11:34:21  
 2009-12-31 11:34:21 interface eth4 is off 2009-12-31 11:34:21  
 2009-12-31 11:34:21 interface eth3 is on 2009-12-31 11:34:21  
 2009-12-31 11:34:21 interface eth3 is on 2009-12-31 11:34:21  
 2009-12-31 11:34:21 interface eth5 is off 2009-12-31 11:34:21  
 2009-12-31 11:34:21 interface eth5 is off 2009-12-31 11:34:21  
 2009-12-31 11:34:21 interface eth6 is off 2009-12-31 11:34:21  
 2009-12-31 11:34:21 interface eth6 is off 2009-12-31 11:34:21  
 总页数: 26 页号: 1



---

3		"	"
4		PC	" "
HTML	CSV	"	"
5			
		IP	IP

The screenshot shows a software interface with a search filter section. At the top, there are buttons for '开始扫描时间' and '结束扫描时间'. Below them is a label '过滤类别选择:' followed by a dropdown menu set to '系统事件' and a radio button for '包含'. Below this is another dropdown menu set to '系统事件' and a radio button for '包含', followed by a '操作:' label and buttons for '搜索' and '运行'. Below the filter section, the text '统计: 647 系统事件' and '时间范围: 全部' is displayed. At the bottom, there is a table with columns 'A', '/', and '00:00:00'.

A	/	00:00:00
---	---	----------

---

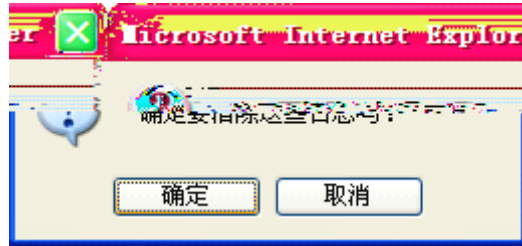
C " "

" "

D " "

" "

" "





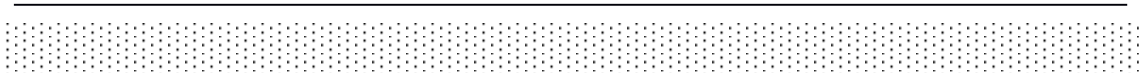
总页数: 1 页号: 1

名称		
urity-rule		

**安全访问规则**  
(总数: 1, 显示: 1-1 of 1)

<input type="checkbox"/>	编号	
<input type="checkbox"/>		default-sec

注释: 点击规则名称可对规则属性进行编辑。



1

2

"

"

3

"

"

WEB

SQL

SQL

WEB

SQL

XSS

WEB

WEB

c

"

"

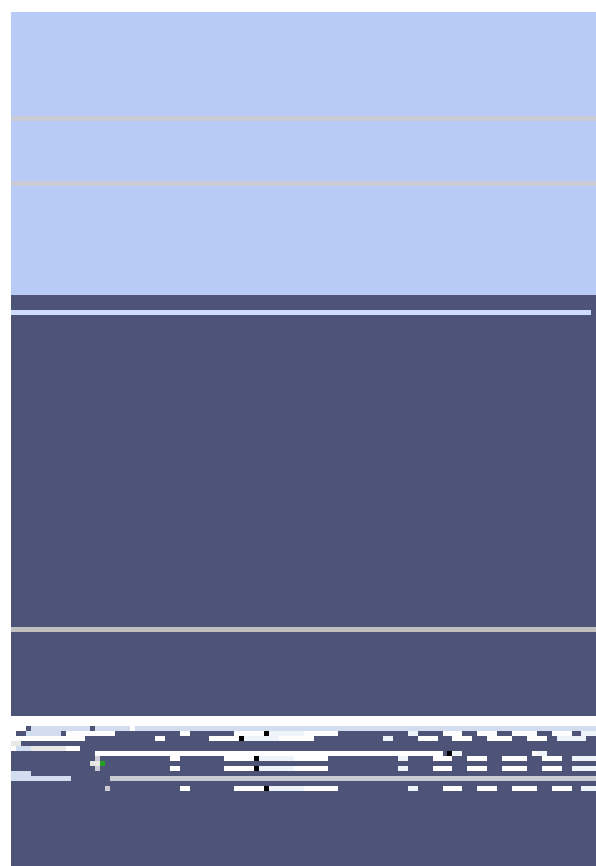
"

"

"

"

3



安全访问规则

(总数: 2, 显示: 1-2 of 2) [删除全部](#)     总页数: 1 页号:

<input type="checkbox"/>	规则名称	名称
<input type="checkbox"/>	1	test
<input type="checkbox"/>	2	

注释: 点击规则名称可对规则属性进行编辑。

5

" " " "

### .1.1

SQL

WEB

SQL

( POST GET)

RG-WG

SQL

SQL

SQL

动作:   启用基本攻击特征库检查

项 动作:   启用扩展SQL注入攻击检查

1

"

"

SQL

" "

2

"

SQL

"

WEB

SQL

" "

3

"

"

SQL



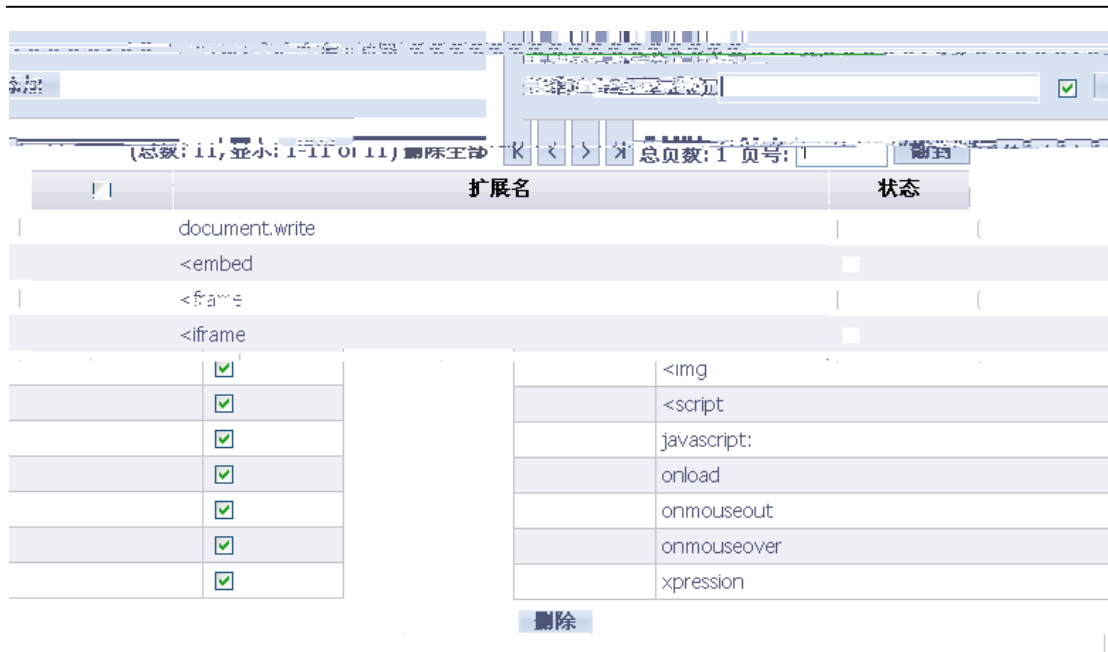
---

A Web

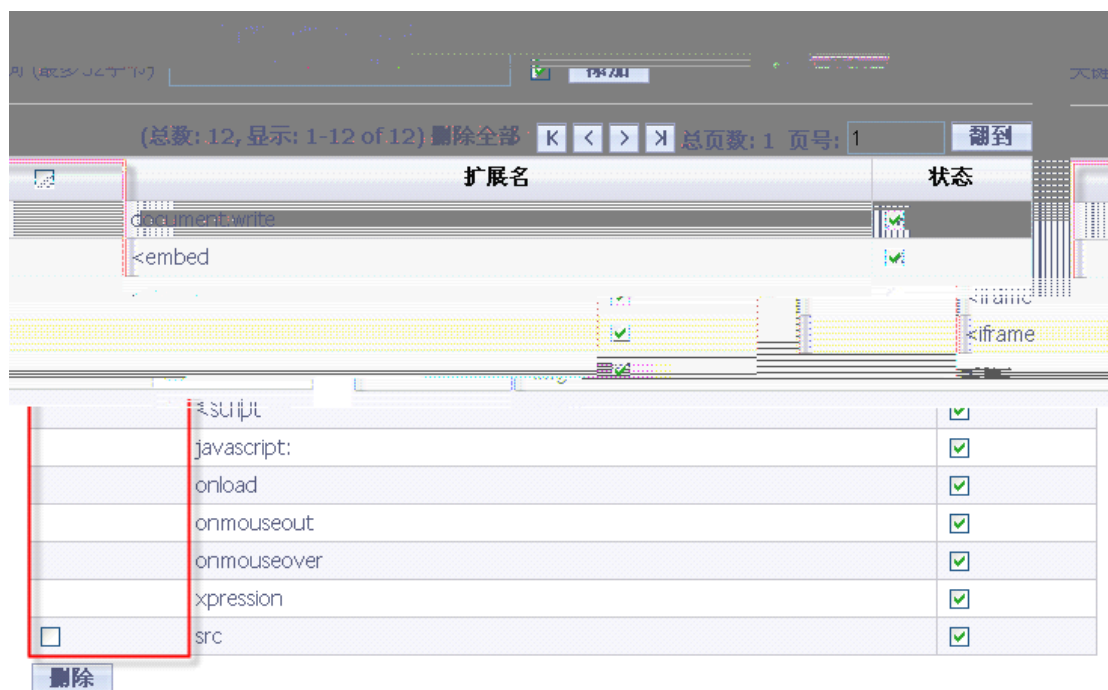
B

CGI

HTML



A



B

---

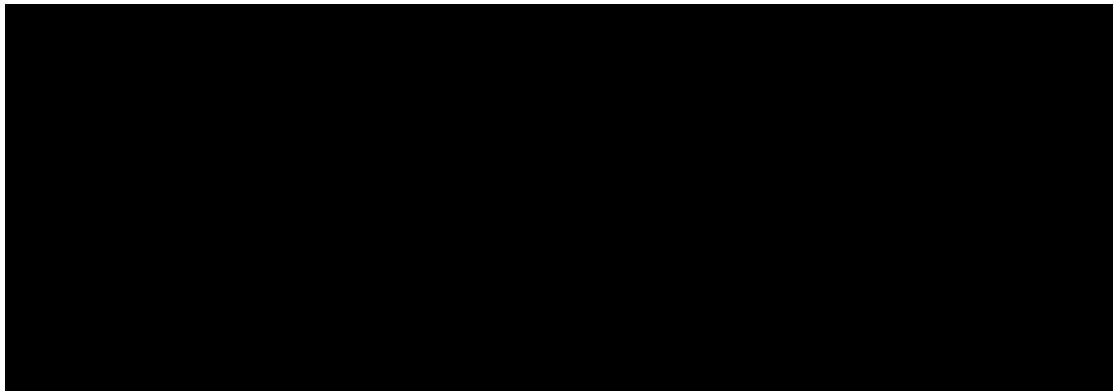
" "

### **.13**

HTML

( )

RG-WG



1 " "

" "

2 " "

3 " "

全部 K [ ] 17/17 删除

数: 17, 显示: 1-17 of 17) 删除全部 K < > X 总页数: 1 页号: 1 翻到 (总数)

扩展名	状态
../	<input checked="" type="checkbox"/>
adduser	<input checked="" type="checkbox"/>
boot.ini	<input checked="" type="checkbox"/>
cat	<input checked="" type="checkbox"/>
cmd	<input checked="" type="checkbox"/>
del	<input checked="" type="checkbox"/>
dir	<input checked="" type="checkbox"/>
eval	<input checked="" type="checkbox"/>
execute	<input checked="" type="checkbox"/>
net user	<input checked="" type="checkbox"/>
passthru	<input checked="" type="checkbox"/>
passwd	<input checked="" type="checkbox"/>
system	<input checked="" type="checkbox"/>
tfpt	<input checked="" type="checkbox"/>
useradd	<input checked="" type="checkbox"/>
userdel	<input checked="" type="checkbox"/>
wget	<input checked="" type="checkbox"/>

删除

后退 刷新

" "

" "

" "

---

4 , 150 password,  
00000,8888  
RG-WG WEB  
" "  
RG-WG  
WEB  
- 2.0 4

扩展名		状态
loginpass	<input checked="" type="checkbox"/>	
login_pass	<input checked="" type="checkbox"/>	
loginpasswd	<input checked="" type="checkbox"/>	
login_passwd	<input checked="" type="checkbox"/>	
loginpassword	<input checked="" type="checkbox"/>	
login_password	<input checked="" type="checkbox"/>	
loginpwd	<input checked="" type="checkbox"/>	
login_pwd	<input checked="" type="checkbox"/>	
pass	<input checked="" type="checkbox"/>	
passwd	<input checked="" type="checkbox"/>	
password	<input checked="" type="checkbox"/>	
pwd	<input checked="" type="checkbox"/>	
txtpass	<input checked="" type="checkbox"/>	
txt_pass	<input checked="" type="checkbox"/>	
txtpasswd	<input checked="" type="checkbox"/>	
txt_passwd	<input checked="" type="checkbox"/>	
txtpassword	<input checked="" type="checkbox"/>	
txt_password	<input checked="" type="checkbox"/>	
txtpwd	<input checked="" type="checkbox"/>	
txt_pwd	<input checked="" type="checkbox"/>	

删除

后退 刷新

**.1.**

WEB

---

RG-WG

WEB

---

启用数据库错误信息检查

动作:

阻止并记日志

"

---

**.1.**

WEB

RG-WG

WEB



" WEB

" RG-WG

WEB

" "

" "

" " " " " "

"

"

**.1.**

RG-WG

WEB

启用危险文件类型下载检查

高级选项

动作:

阻止并记日志

1

"

"

RG-WG

"

"

WEB

"

"

"

"

"

"

"

"

"

"

"

"

2

与下载相关的危险文件类型表

扩展名 (最多32字节)



添加

<input type="checkbox"/>	扩展名	状态
<input checked="" type="checkbox"/>	mdb	<input checked="" type="checkbox"/>
<input type="checkbox"/>	tar	<input checked="" type="checkbox"/>
<input type="checkbox"/>	zip	<input checked="" type="checkbox"/>

后退

刷新

" mdb"

WEB

RG-WG

" mdb"

WEB

A

"

"

"

"

B

"

"

C

"

"

"

"

RG-WG

**.1.**

RG-WG

WEB

WEB

启用危险文件类型上传检查

高级选项

动作:

阻止并记日志

---

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

WEB  
WEB

---

WEB

A

" " " "

B

" "

C

" " " "

RG-WG

**.1.10**

" IP "

WEB

RG-WG

" IP "

IP

IP IP

有权访问的IP列表

页号:

IP/掩码

A

IP

"

IP

"

IP

"

"

禁用语列表  
 关键词 (最多32字节)   
 应用域  URL  URL参数  Cookie  POST

XST表单 **添加**

K < > K 页号: 1 翻到

URL参数  Cookie  POST表单

**删除**

<input type="checkbox"/>	关键词	URL <input checked="" type="checkbox"/>
<input type="checkbox"/>	关键词	URL <input checked="" type="checkbox"/>

A

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

删除全部 K < > K 1 翻到

<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"/>

**删除**

B

C

" Cookie" Cookie

翻到 (总数: 2, 显示: 1-2 of 2) 删除全部 K < > K 总页数: 1 页号: 1

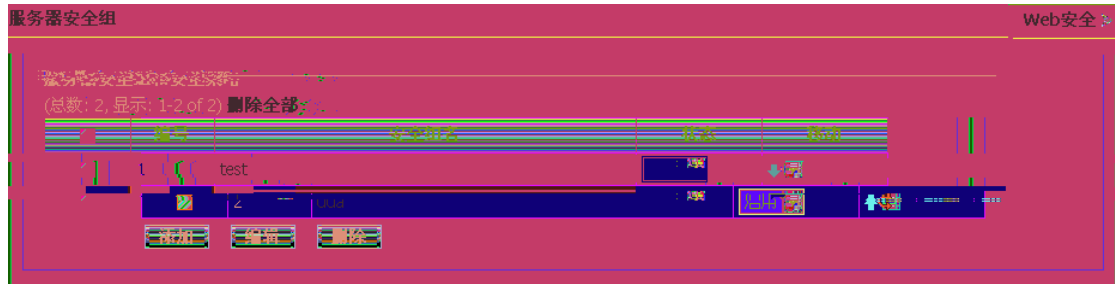
<input type="checkbox"/>	关键词	URL <input checked="" type="checkbox"/>	URL参数 <input type="checkbox"/>	Cookie <input checked="" type="checkbox"/>	POST <input type="checkbox"/>
<input type="checkbox"/>	关键词	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Cookie	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**删除**

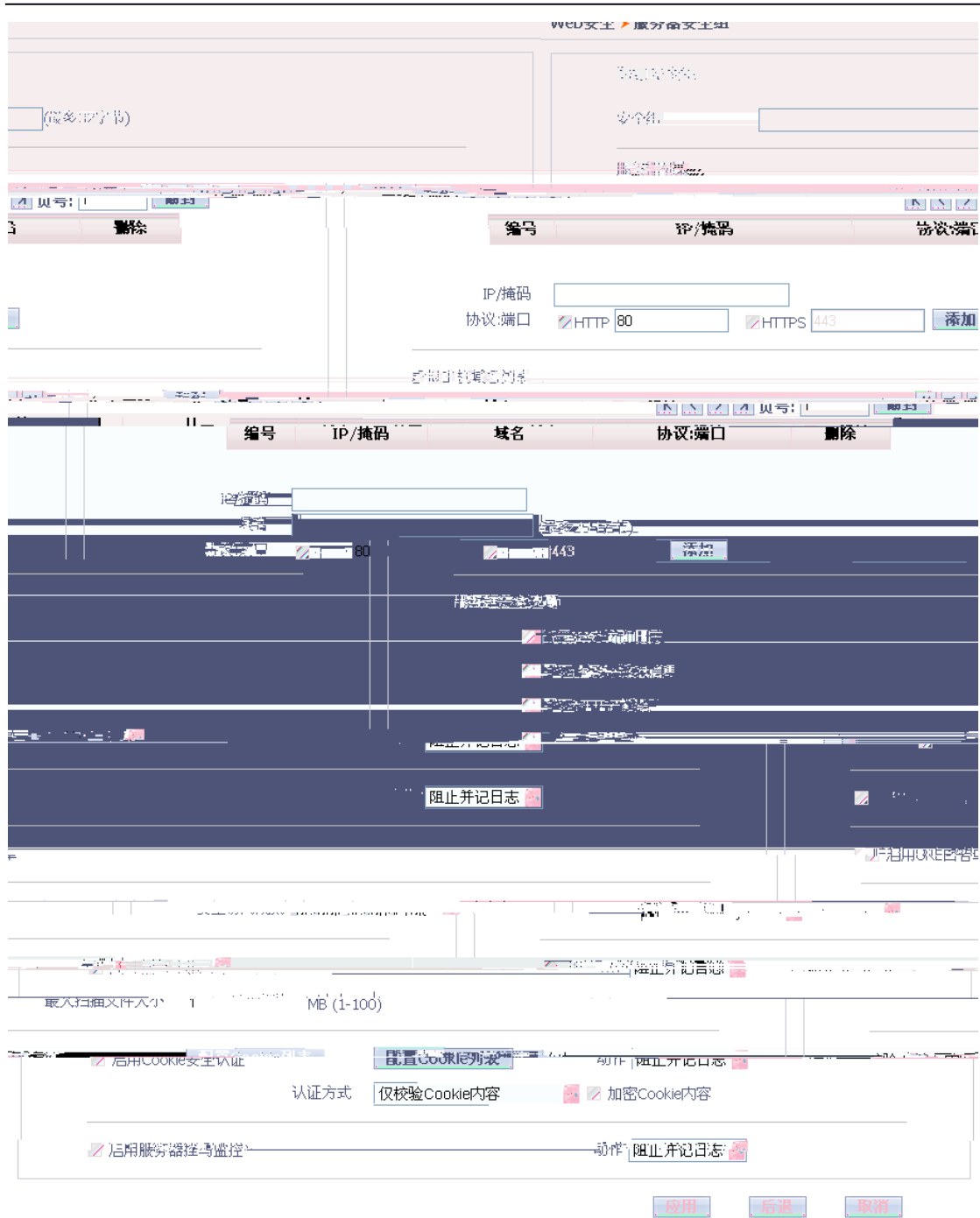
.2

## WEB

1



" "



A " " " " "

" WEB IP

WEB

B " " WEB

WEB HTTP

" " " "

---



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](#)

状态	移动	编号	名称
<input type="checkbox"/>		1	default-gropu
<input type="checkbox"/>		2	1
<input type="checkbox"/>		3	123
<input type="checkbox"/>		4	2
<input type="checkbox"/>		5	3
<input type="checkbox"/>		6	4
<input type="checkbox"/>		7	6
<input type="checkbox"/>		9	8
<input type="checkbox"/>		10	9
<input type="checkbox"/>		11	10
<input type="checkbox"/>		12	11
<input type="checkbox"/>		13	12
<input type="checkbox"/>		14	
<input type="checkbox"/>		15	14
<input type="checkbox"/>		16	5
<input type="checkbox"/>		17	15
<input type="checkbox"/>		18	16
<input type="checkbox"/>		19	11
<input type="checkbox"/>		20	19
<input type="checkbox"/>		21	17
<input type="checkbox"/>		22	21
<input type="checkbox"/>		23	21
<input type="checkbox"/>		24	22
<input type="checkbox"/>		25	23

启用  禁用  启用  禁用

" "



安全组 Web安全 > 服务器安全组

1

方向

" " " " " "

" "

" 1" " default-grou"

## .2.1

### WEB

1 " " WEB IP

The screenshot shows a configuration page with a table and a form. The table has columns for IP, protocol/port, and delete. The form below has fields for IP/mask, protocol (HTTP/HTTPS), and port (80/443).

IP	协议端口	删除	编号
192.168.1.1	HTTP:80	删除	1
192.168.1.2	HTTP:80	删除	2
192.168.1.3	HTTP:80	删除	3
192.168.1.4	HTTP:80	删除	4

IP/掩码:

协议端口:  HTTP 80  HTTPS 443

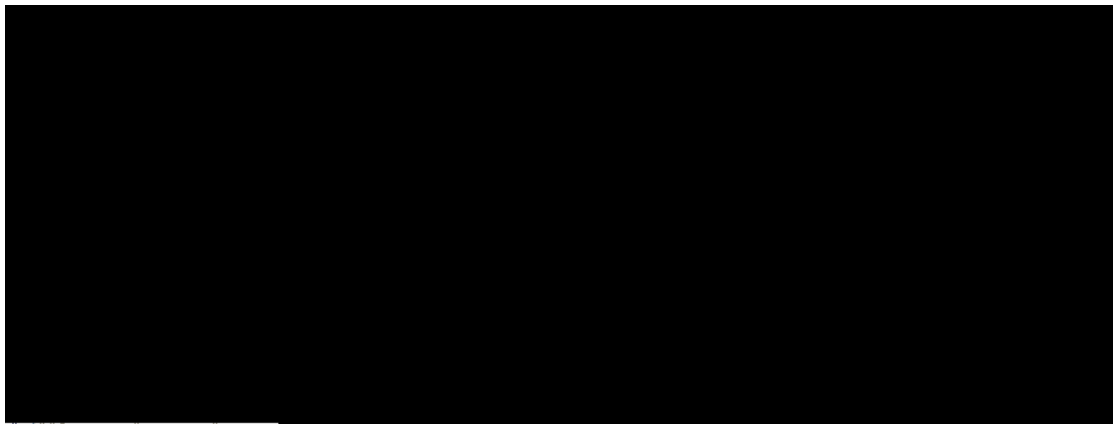
" IP/ " WEB IP WEB

" "

" "

2 WEB " "

WEB IP



协议端口:  HTTP 80  HTTPS 443

---

" IP/ " WEB IP " " WEB  
" " " " WEB  
" "

" "  
" "

HTTP

配置防溢出检查

URL最大长度	<input type="text" value="2048"/>	(0-65536) 字节
URL参数个数	<input type="text" value="100"/>	(0-1000)
URL参数内容最大长度	<input type="text" value="1024"/>	(0-65536) 字节
POST表单个数	<input type="text" value="100"/>	(0-1000)
POST表单内容最大长度	<input type="text" value="65536"/>	(0-1048576) 字节
Cookie个数	<input type="text" value="200"/>	(0-200)
Cookie内容最大长度	<input type="text" value="4096"/>	(0-65536) 字节

应用

后退

取消

URL	URL 0-65536 2048 URL ( [] ) protocol :// hostname[:port] / path / [;parameters] [?query] #fragment URL " // " http://www.sina.com.cn/ URL 16
URL	URL 0-1000 100 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
URL	URL 0-65536 1024 URL URL / (?) name=value URL (&) URL = &
POST	POST 1-1000 100
POST	POST 65536 0-1048576 post
Cookie	WEB cookie

	200	0-200
Cookie	WEB 4096	cookie 0-65536

" "

## .2.3

" URL " WEB URL

" URL " URL RG-WG

1

2

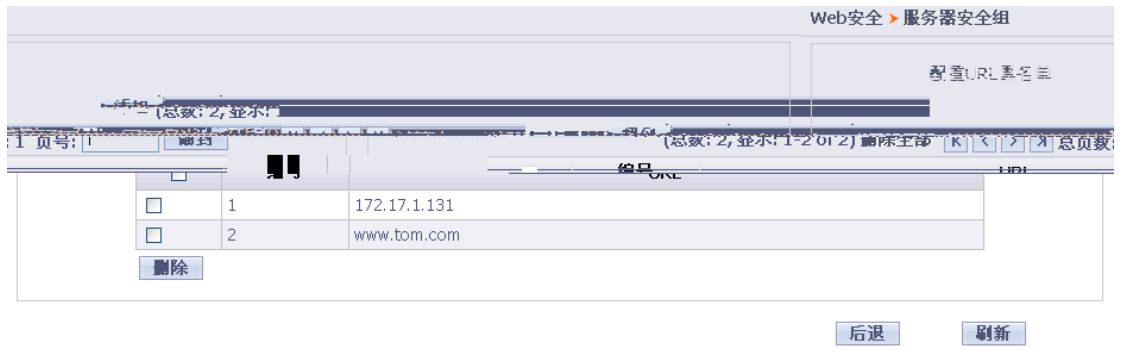
WEB URL

URL URL

A " " URL



B " " URL URL



" URL " WEB URL path level  
 URL " "

www.sina.com URL  
 " "

WEB WEB URL  
 URL URL URL URL  
 URL

A " " URL

启用URL白名单(不做任何安全URL)

B " " URL URL URL  
 URL



" URL " WEB URL path  
 level URL " "  
 www.sina.com URL  
 " "

## .2.4

Web

URL

## 5.1

1 WEB

安全访问规则 default-security-rule

2

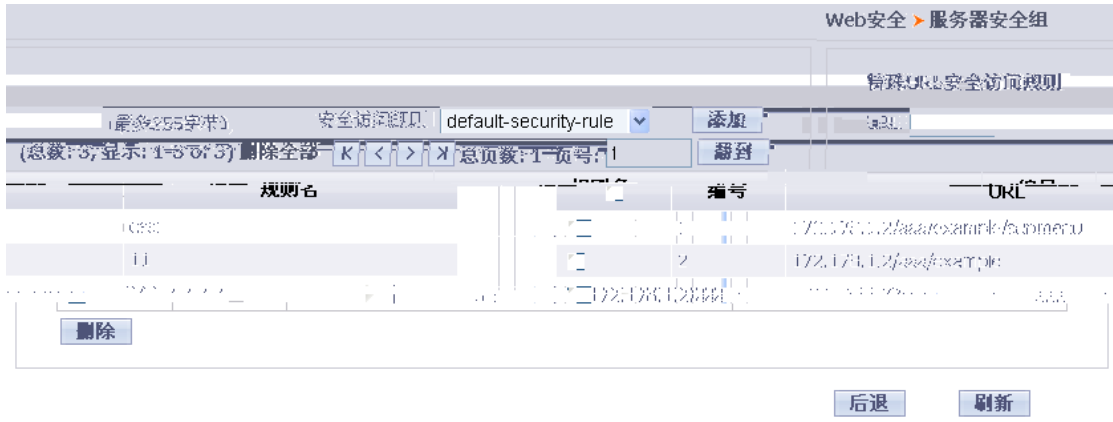
URL

Web安全 > 服务器安全组



A

" URL" URL " "  
 " " " "



B

" "

## 2.

RG-WG

WEB

1

" " "

" RG-

WG WEB

" "

启用上传病毒扫描

动作 阻止并记日志

最大扫描文件大小  MB (1-100)

1

WEB

2

WEB

3

WEB

2

100 M

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

cookie list cookie

Web安全 > 服务器安全组

配置Cookie列表

(最多32字节)

页号:

<input type="checkbox"/>	编号	Cookie
<input type="checkbox"/>		

## .2.

RG-WG	WEB	WEB
1	"	"

启用服务器挂马监控

高级选项

动作

阻止并记日志

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

1 WEB

2 WEB

3 WEB

,

2 " "

RG-WG

" "



IP " "

" "

---

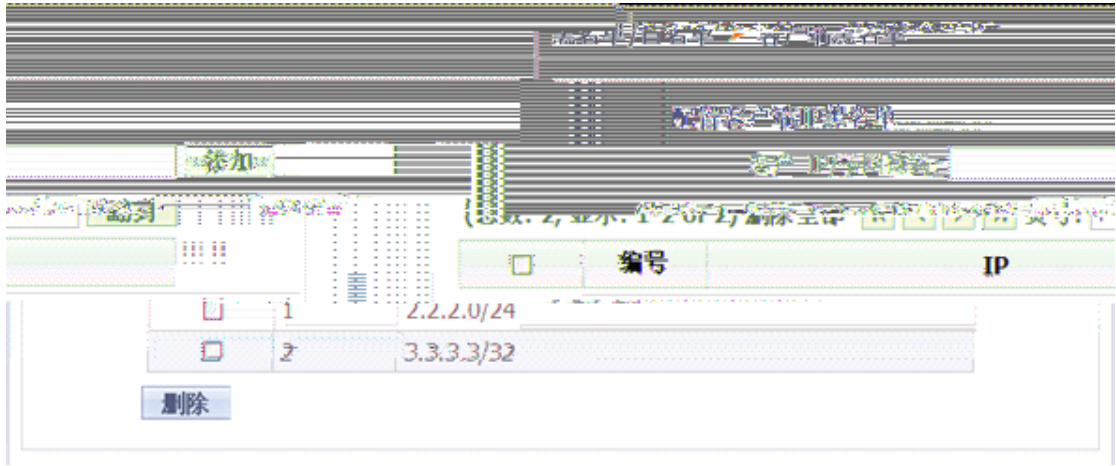
/

RG-WG	"	"	RG-WG
WEB	"	"	"
"	RG-WG	IP	WEB
	"	"	WEB
IP	RG-WG	HTTP	
1			
2			
3			
4			
5	IP		
6	"	"	URL
7	"	"	URL
8	"	"	IP

**.1**

IP WEB

1 /



2

" IP " IP " "

3

" "

## .2

Ruijie RG-WG

IP WEB

SQL

" block" RG-WG

IP

WEB

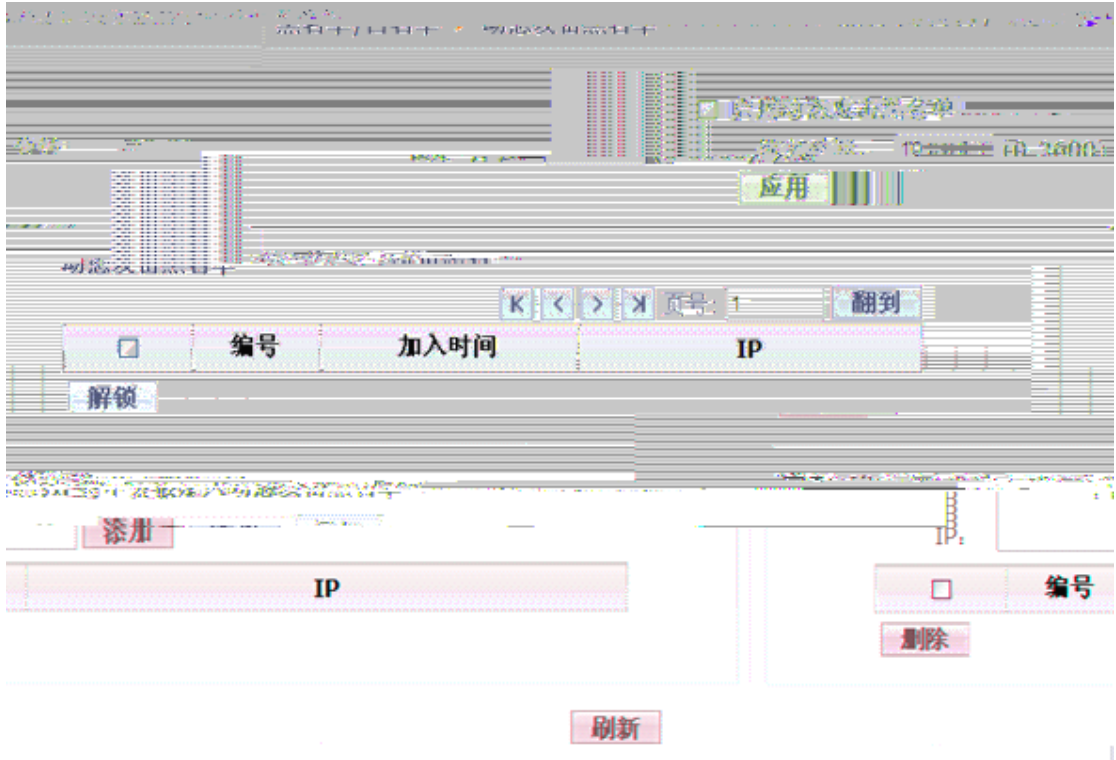
IP

IP

WEB

1

/



2

" " IP  
 IP "

WEB

10

RG-WG

IP

3

10 " "

4

" " IP " " IP

5

IP

IP

IP

IP

### .3

IP

WEB

1 /

黑名单/白名单 > 客户端白名单

配置客户端IP白名单

客户 IP/子网掩码:

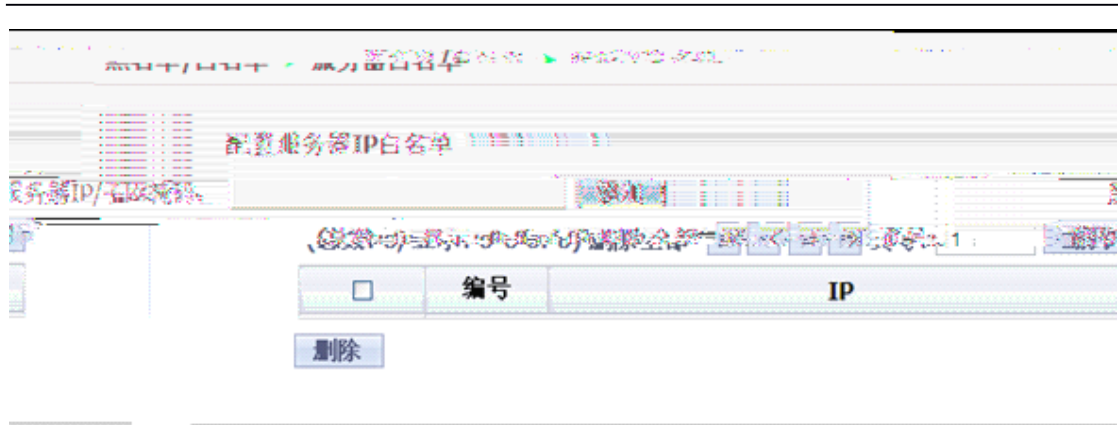
页号:

<input type="checkbox"/>	编号	IP
<input type="checkbox"/>	1	2.2.2.2/32

2

" IP " IP " ' "

3



2

" IP/ " IP

" "

IP " "

" "

3

" "

---

# .1

## .1.1

RG-WG

WEBUI

" %

1

系统设置 > 语言

管理

语言: 简体中文

应用 取消

---

2 " "

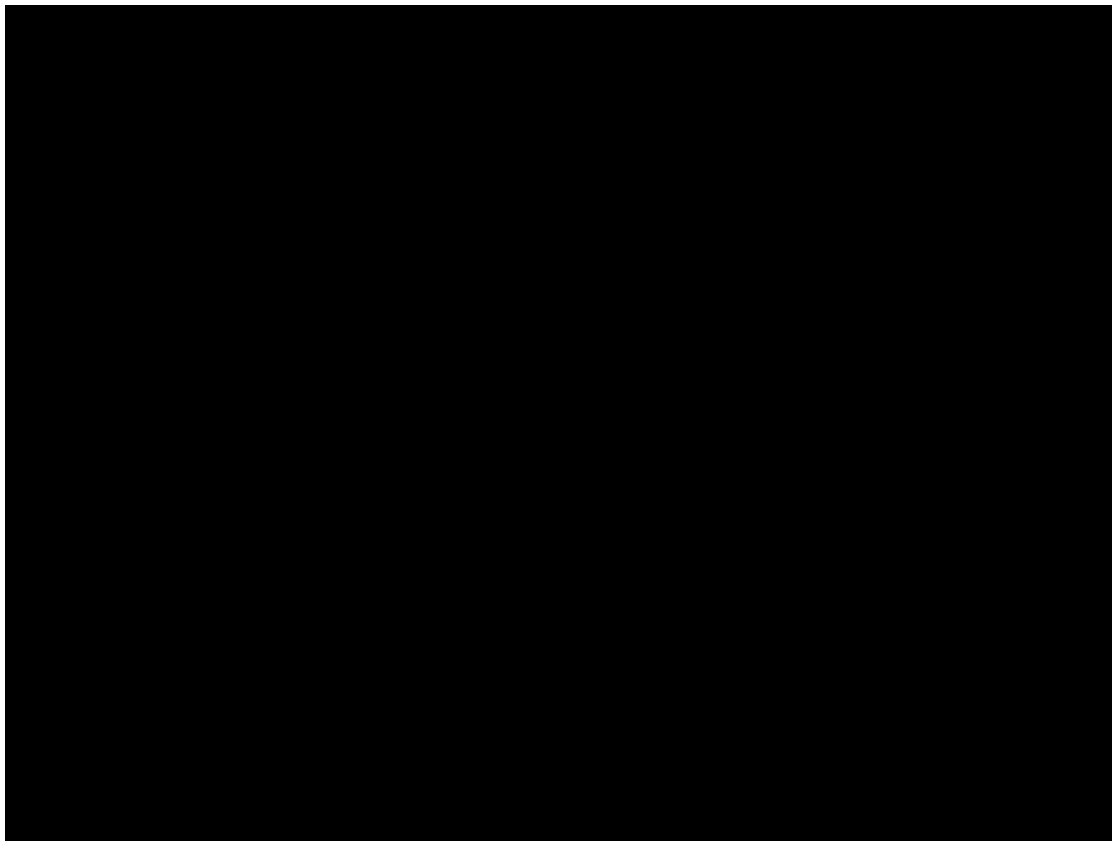
3 " "

## **.1.2**

SNMP SNMP

NTP

DNS



应用 取消

### **.1.2.1**

" "

---

" "

' -

" "

### **.1.2.2**

		SNMP polling	SNMP
1	" SNMP"		
2	" Community"	SNMP	SNMP
		SNMP	
3	SNMP		

日期: 2009年12月21日 星期一 11:38:38 AM

手动设置日期/时间为

年: 2009 月: 12 日: 21

时: 17 分: 11 秒: 38

时区: +8

启用 NTP

服务器名称: north-america-pool.ntp.org

自动同步时间间隔: 60 (12-180 分钟)

```

" " WEBUI " "
1
" "
2 NTP
" NTP "
NTP
NTP
" " NTP
" "

```

---

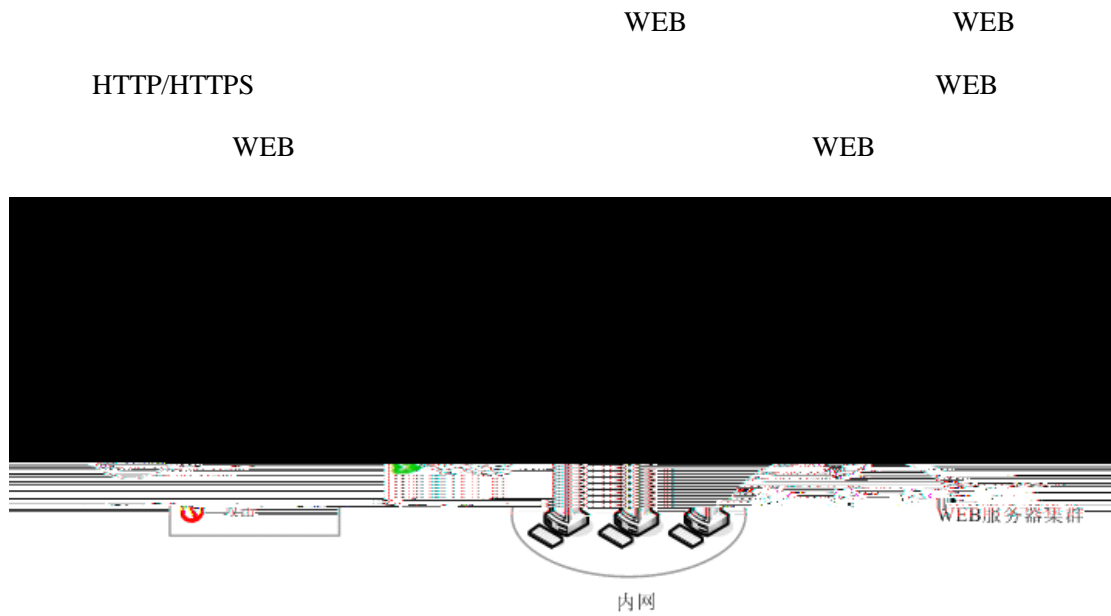
首选DNS服务器

备选DNS服务器

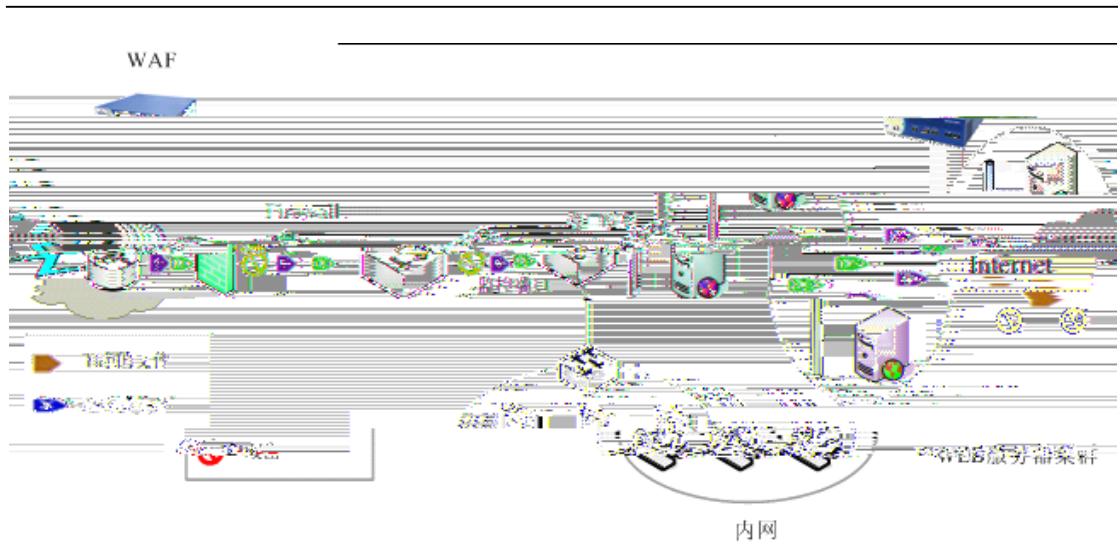
“ ”

## .1.3

### .1.3.1



SPAN



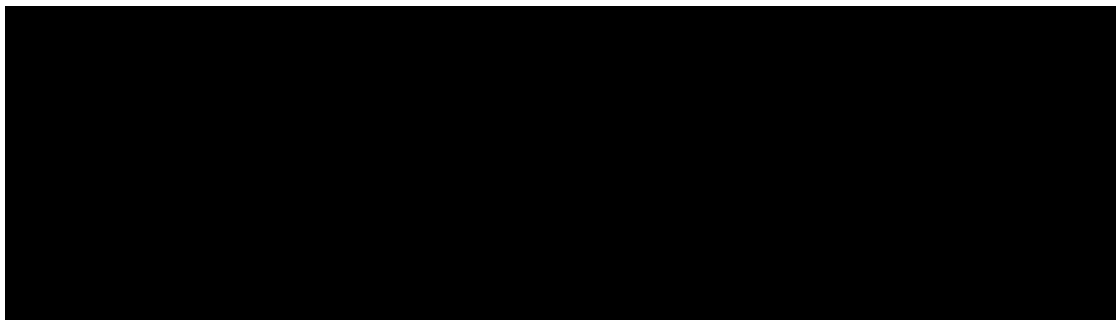
span

WEB

WEB

1

2



3

“ ”

4

---

### .1.3.2

RG-WG

bypass

failopen

WEB

1

对于通过策略匹配到内容过滤策略的流量，如果策略配置了 fail-open 策略，则流量将被旁路处理，而对于匹配到通过策略或者其他流量则不生效。

- Fail-open: 旁路匹配到内容过滤策略的新建连接。
- Fail-close: 阻断匹配到内容过滤策略的新建连接。

2

Fail-open

WEB

Fail-close

WEB

3

" "

### .1.3.3

Ruijie RG-WG

HTTP/HTTPS

"

"

Ruijie

WEB

1

2

" "

---

## ■ 零日防护计划

加入锐捷零日防护计划将进一步提高您的网络安全性。锐捷web安全网关将会把所检测到的可疑请求自动提交到锐捷安全实验室。锐捷安全实验室的零时威胁检测系统将迅速分析和处理提交的相关数据，并及时提供升级更新服务，使客户网络免受潜在威胁的侵害

3 " "

### .1.3.4

TCP TCP  
TCP  
1  
2 " 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，有效提高系统安全性。

3 " "

### .1.4

WEB  
HA QMAIL  
1

发送邮件地址	<input type="text"/>
接收邮件地址	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
<hr/>	
<b>邮件转发服务器设置:</b>	
转发服务器地址或名称	<input type="text"/>
	<input type="checkbox"/> 服务器要求安全传输 (SSL)
端口	<input type="text"/> (0-65535)
<input checked="" type="checkbox"/> SMTP 认证	
SMTP 用户名	<input type="text"/>
密码	<input type="text"/>
<hr/>	
使用邮件转发服务器	<input type="checkbox"/> 告警邮件 <input type="checkbox"/> 报表邮件 <input checked="" type="checkbox"/> 隔离邮件

应用

取消

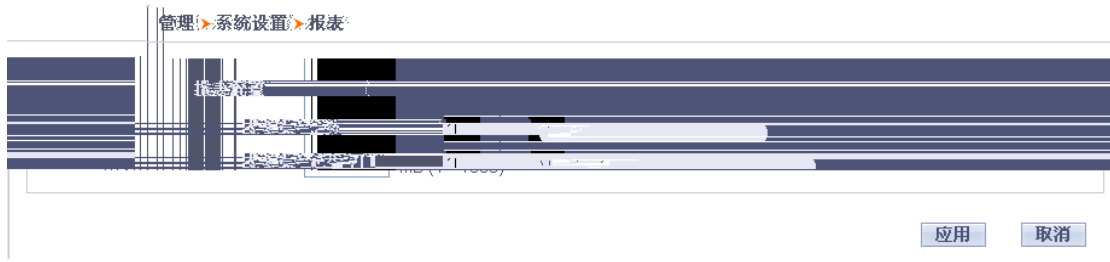
2



“ ”

.1.

1



2 " " 1-60

3 " " 1-1000 ( MB)

4 " "

## .1.

FTP Syslog

### .1. .1

FTP

1

FTP

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 (30-365)

最大磁盘空间  (5000-50000) MB

最大使用率  %

日志满操作

---

**日志** 启用系统

管理事件

系统事件

Web应用防火墙

客户端黑名单

动态攻击黑名单

---

日志计划将日志定时导出到外部服务器。  
 导出

设置  按星期

按天数 每隔  天 (1-30)

导出时间  (hh:mm)

导出日志  
 为避免日志丢失，定制脚本操作将导出所有类别的启用日志  
 导出定时

---

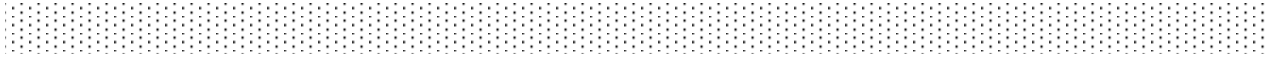
导出日志到FTP服务器

密码

导出后删除本地日志

2

	5000-50000 MB
	1 - 100
	<p>1 <span style="margin-left: 150px;">4.2.4</span></p> <p>2 <span style="margin-left: 150px;">HA</span></p> <p>3 WEB <span style="margin-left: 100px;">4.2.5</span> <span style="margin-left: 150px;">WEB</span></p>



4

IP WEB

5

IP WEB

SQL

" b

3

FTP

"

"

"

"

FTP

FTP

4

"

"

## **.1. .2**

Ruijie RG-WG

Syslog

Syslog

Ruijie RG-WG

7



2 Syslog " Syslog "  
Syslog

WEB HA  
WEB

3 Syslog  
Syslog Syslog  
IP IP

" " " " " " " " " Syslog  
syslog

7 7 0

4 " "

## .1.

RG-WG SNMP Trap HA  
" " 7.1.4

### .1. .1

RG-WG HA HA  
" " WEB

1

管理 > 系统设置 > 警告通知 > 邮件警告

- 启用HA警告
- 启用许可证警告

距许可证过期天数  (1-30 天)

2 HA " HA "

3 " "

4 " "

### .1. .2

SNMP SNMP trap SNMP

SNMP v1 v2 SNMP 7.1.2.2

SNMP

SNMP SNMP trap SNMP

1



---

RG-WG  
IP

IP

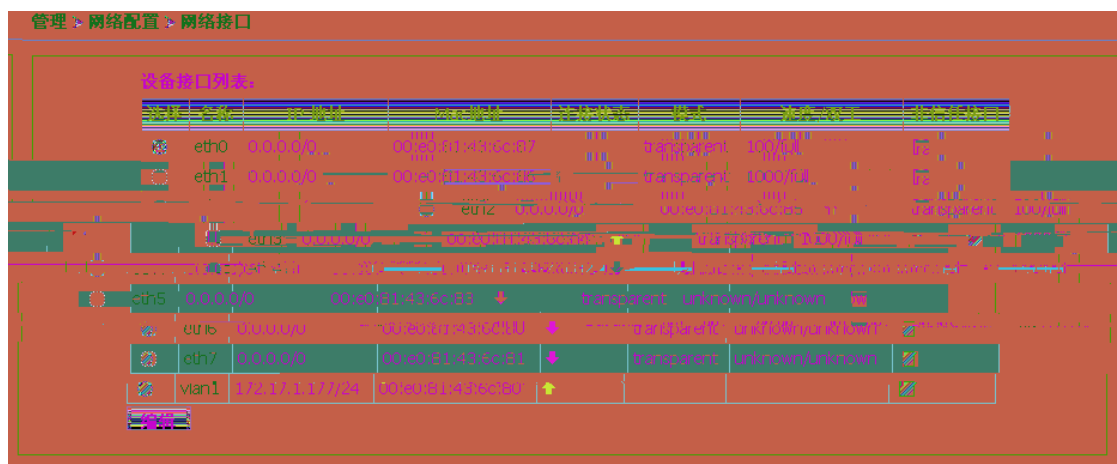
### **.2.1.1**

RG-WG

.

RG-WG

RG-WG



## VLAN

### .2.1.3

eth0

IP地址/子网掩码

接口模式  透明  路由

---

HTTPS  SSH  Ping  SNMP  
 Up  Down  
 自适应  
 固定

速率  MB

双工

应用 取消

IP /	IP
	" " " "
	HTTPS SSH PING SNMP
" Up"	/ " Down"
	10 100 1000 MB

" "

## .2.2

(VLAN)

LAN IEEE 802.1Q

LAN

VLAN

VLAN ID

R & D

ID

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

802.1Q

VLAN

VLAN

VLAN

VLAN 1

VLAN

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				

VLAN 1

VLAN 1

" Native VLAN" " "

### .2.3

MAC

MAC

1

配置 > 静态MAC地址

管理 > 网络

静态MAC记录:

页号:  翻到

<input type="checkbox"/>	Mac地址	VLAN	接口
<input type="checkbox"/>			

2

管理 > 网络配置 > 静态MAC地址

新建静态MAC记录:

Mac地址  (e.g. 00:2c:1a:2b:3e:1f)

VLAN

接口

应用

取消

MAC	MAC
VLAN	MAC VLAN
	MAC

3 " "

ARP

IP

ARP

ARP

Ruijie

1

管理 > 网络配置 > ARP探测

ARP Probe记录		
(总数: 2, 显示: 1-2 of 2)		
K < > X 总页数: 1 页号: 1		
<input type="checkbox"/>	目标IP地址	VLAN
<input type="checkbox"/>	172.17.1.177	1
<input type="checkbox"/>	192.168.11.136	1

2

ARP

"

IP

"

IP

" VLAN"

IP

VLAN

3

ARP

"

"

管理 > 网络配置 > ARP探测

新建ARP probe:

ARP Probe记录

VLAN

应用

取消

" ARP Probe "

IP

IP

# ICMP

1

管理 > 网络配置 > 路由表

(总数: 2, 显示: 1-2 of 2)

<input type="checkbox"/>	编号	目的	子网掩码	网关	接口
<input type="checkbox"/>	1	172.23.1.0	255.255.255.0	直连	vlan1
<input type="checkbox"/>	默认	0.0.0.0	0.0.0.0	172.23.1.1	vlan1

" " " "

0.0.0.0

2

A " "

管理 > 网络配置 > 路由表

添加新的路由记录:

添加为默认网关

目的

子网掩码

网关

" "

" " IP

" "

" " IP IP

B " "

---

3

A " " " "



" " IP IP

B " "

" "

## **.2.**

RG-WG

Virtual Router Redundancy Protocol

VRRP

### **.2. .1**

RG-WG

VRRP

VRRP

HA

VRRP

RG-WG

1

3

VRRP

2

---

Down

VRRP

3

ping

VRRP

4 RG-WG

7.2.6.5 HA

5 "

ster

**设置Failover**

---

0.0/0

(1-254) 设置254将成为主机

(1-254) 1为默认值

(1-30) 秒

0.0

---

(1-10) 秒

(1-32)

加保护: (1-32)

加保护: (1-32)

加保护: (1-32)

---

eth0

eth1

eth2

eth3

eth4

eth5

eth6

eth7

---

启用先白模式: 先占延的: (0-500) 秒

启用HA

HA状态 **Ma**

Failover状态 No

MAC Block

---

集群IP地址/掩码 0.0

HA接口

HA优先级 100

组ID 1

保持间隔 1

对等IP 0.0

启用设备故障切换临界值

---

跟踪时间 3

设备切换临界值 32

跟踪1 接口地址 1#

跟踪2 接口地址 2#

跟踪3 接口地址 3#

---

应用 取消

2&

&

---

HA

B " HA "

HA

254

1-254

C " ID" HA ID

ID

HA

HA

ID

**4**

A " HA "

1

eth3

HA

eth3

2

HA

"

"

IP

B " IP "

IP

HA

IP

C " "

" Failover"

HA

" Failover"

"

"

"

"

---

启用	接口名称	加权系数 (1-32)
----	------	-------------

<input checked="" type="checkbox"/>	eth0	<input type="text"/>
<input type="checkbox"/>	eth1	<input type="text"/>
<input type="checkbox"/>	eth2	<input type="text"/>
<input type="checkbox"/>	eth3	<input type="text"/>
<input type="checkbox"/>	eth4	<input type="text"/>
<input type="checkbox"/>	eth5	<input type="text"/>
<input type="checkbox"/>	eth6	<input type="text"/>
<input type="checkbox"/>	eth7	<input type="text"/>

A " "

B " "

HA

1-32

VRRP

UP

Master



---

Master

0 600 " 0"

" "

## **.2. .3**

HA pair

WEBUI IP

HA

CLI

WEBUI







---

3

"

b " " " " " WEB  
 " " "

5

a

b " " " " " WEB  
 " " " " "

6

回到到先前的病毒特征库

回到到先前的WEB应用防火墙特征库

应用

" " " " WEB "

" " " " " "

Web " " 1042.11

1000.41 " " 1042.11

" WEB " RG-WG

1000.41

更新状态:

更新	版本	先前版本	最近更新时间	状态
病毒特征库	1042.13	1042.11	2010.01.28 09:07	updated
Web应用防火墙特征库	1000.43	1000.41	2010.01.28 09:10	up to date

### .3.1.3

1

认证机制  None-auth  Basic  NTLM

系统将发送以下的证书到认证服务器

域 (只用于NTLM认证)

认证服务器IP地址

端口  (1-65535)

用户

密码

	<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 " "

### .3.2

WEB

RG-WG

WEB

“ ”

License  
WG License  
License License  
License  
1

管理 > 系统维护 > 许可证

许可证状态

许可证	状态	有效日期
病毒库许可证	有效	2009.01.01 - 2012.01.01
Web应用防火墙许可证	有效	2009.01.01 - 2012.01.01

更新许可证

2  
“ ” “ ”

### .3.3

WEBUI RG-WG

1

管理 > 系统维护 > 系统重启

操作类别

2 “ ”  
3 “ ”

---

## .3.4

“ ”

1

管理 > 系统维护 > 拨号支持

生成与导出技术支援文件

系统支持文件包括内部生成的帮助doc文件、有用于ruijie技术人员的问题解决方案、  
生成文件，保存文件名称的生成帮助ruijie技术和设备名称。

生成这个文件文件

2

“

”

3

PC

## .4

RG-WG

administrator

administrator

WEB

CLI

### .4.1

WEBUI CLI

RG-WG

---

“ administrator”

“ administrator”

9

1

管理 > 访问管理 > 用户账号

<input type="checkbox"/>	编号	权限	管理员名称
	1	Read-Write	administrator
<input type="checkbox"/>	2	Read-Write	liyune

2

“ ”

管理 > 访问管理 > 用户账号

名称

密码

确认新密码

权限  Read-Write  Read-Only  Audit

	“ ”
	Read-write —

	Read-only ---
	Audit ---

3 " "

## .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
	10	5
	"	"

	5-30	5
HTTPS	HTTPS	443
SSH	SSH	22
		IP
	" "	IP " "

3 " "

WEBUI

3 syslog

" [Syslog](#) "

---

Syslog

**.2**

/IP

---

IP WEB IP  
 IP WEB IP  
 URL URL

block\_log

log

Logcategory=Malware\_Alert Protocol=HTTP Client\_IP=<ip\_address>

Server\_IP=<ip\_address> Http\_Method=<GET|POST> URL=<URL>

Malware=< Malware Name> Action=<Blocked | Quarantined>

### .3.2

WEB

sp\_attack

IP WEB IP  
 IP WEB IP  
 WEB GET  
 URL POST  
 URL URL  
 URL POST

Cookie

" " " "

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



---

Action=Adjust time from NTP server 67.18.187.111 offset 0.026822 sec