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

“ ”

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 1.50 1.50

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

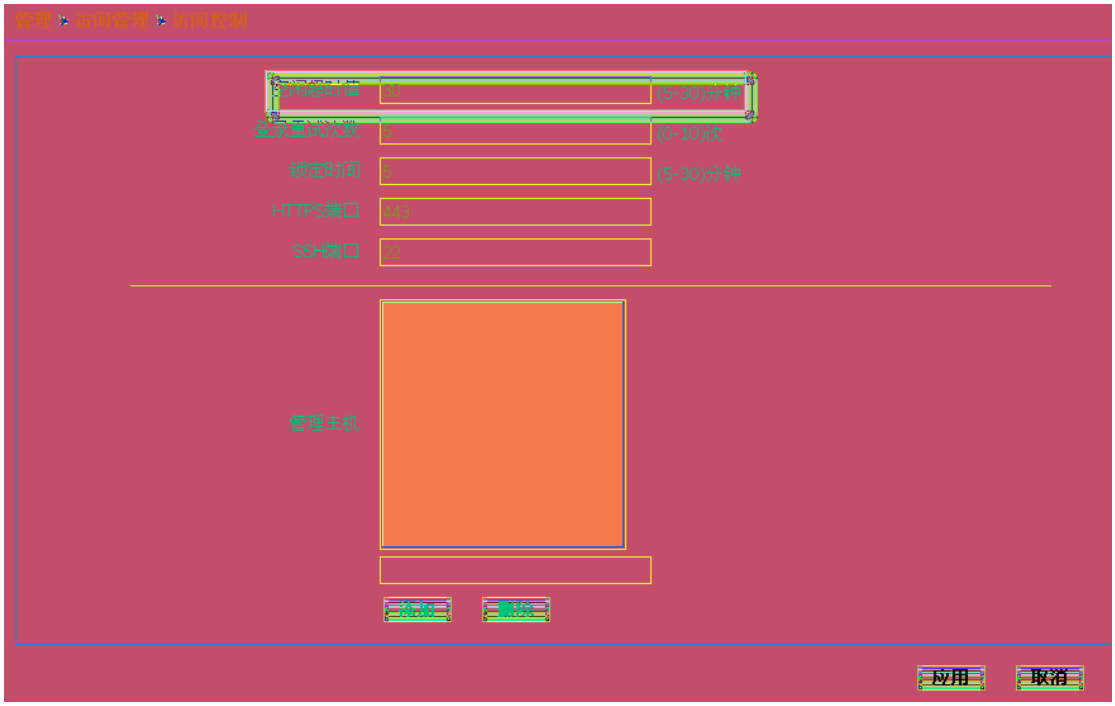
4 “ ”

“ ”

2.2

WEBUI

WEBUI


管理 ▸ 访问管理 ▸ 访问控制
会话超时值
30
(5-30)分钟
登录最大次数
0
(0-10)次
锁定时间
0
(5-30)分钟
HTTPS端口
443
SSH端口
22
管理主机
添加
删除
应用
取消

3

3.1

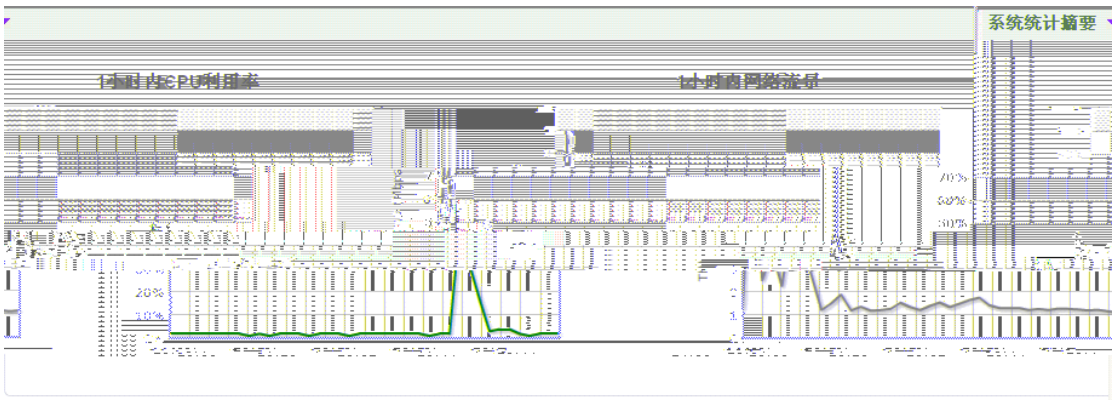
1


CSG20002000306
3.20.0.WAF.19 [更新]
1042.51 [更新]
有效(2009.01.01 - 2012.01.01)
特征库版本: 1000.44 [更新]
许可证: 有效(2009.01.01 - 2012.01.01)
主机名: 177
运行时间: 1 天 1 小时 8 分钟
CPU利用率: 1%
内存利用率: 16%
日志存储空间利用率: 0%
监控模式: Preventative
HA状态: Standalone
序列号:
系统版本:
病毒特征库版本:
病毒库许可证:
Web应用防火墙
Web应用防火墙
系统统计摘要
1小时内网络流量
1小时内CPU利用率
10%
0%
10:34
10:46
10:58
11:10
11:22
(Mbps)
0
10:34
10:46
10:58
11:10
11:22

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

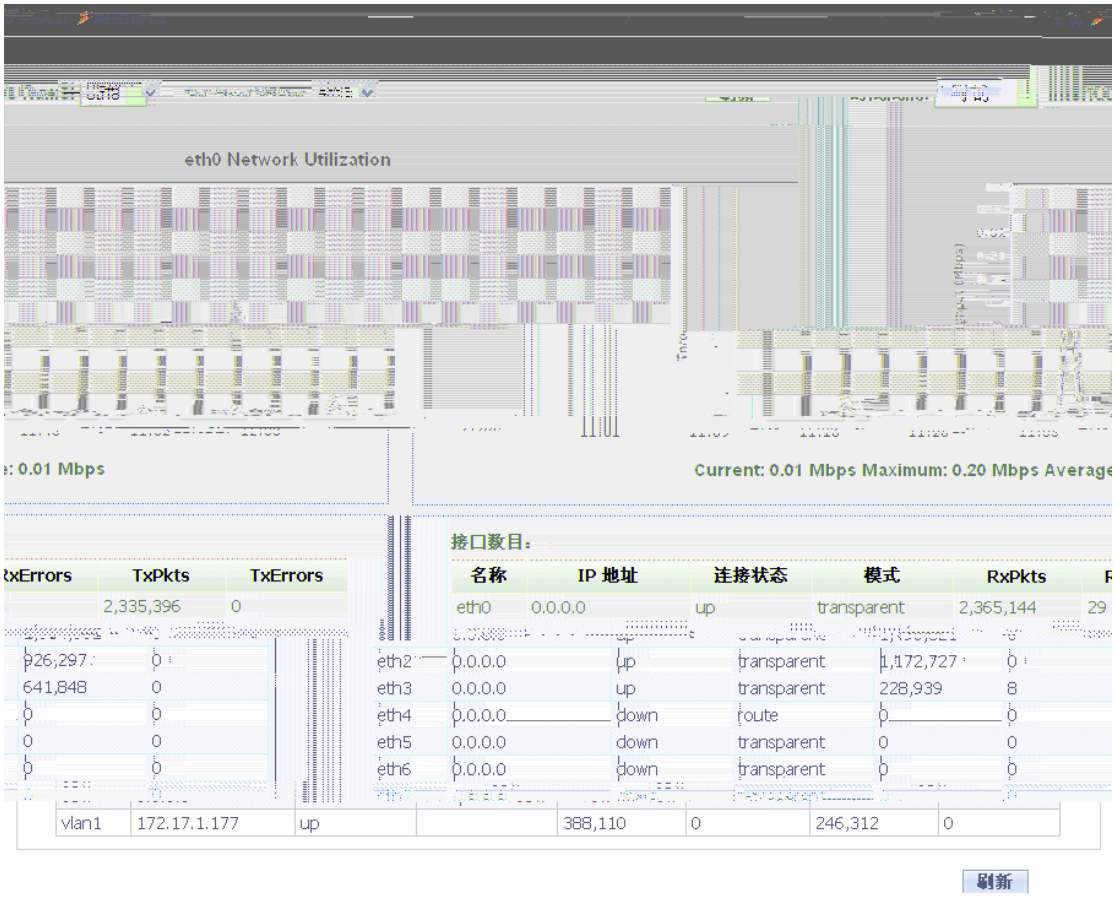
CPU

“ ”

“ ”

“ ”

3.2.2



IP	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

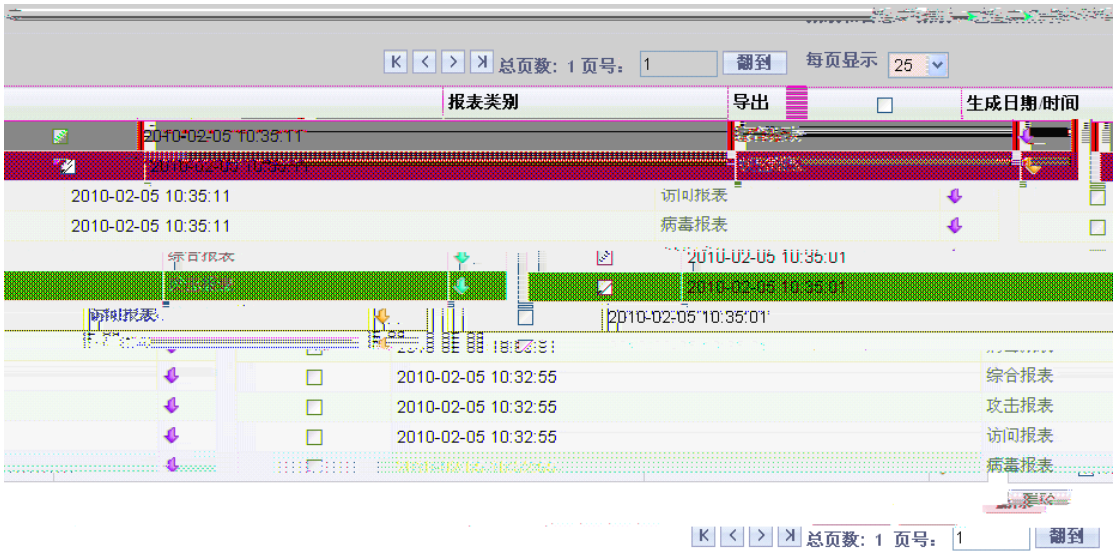
“ ”

“ ”

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

“ ”

“ ”

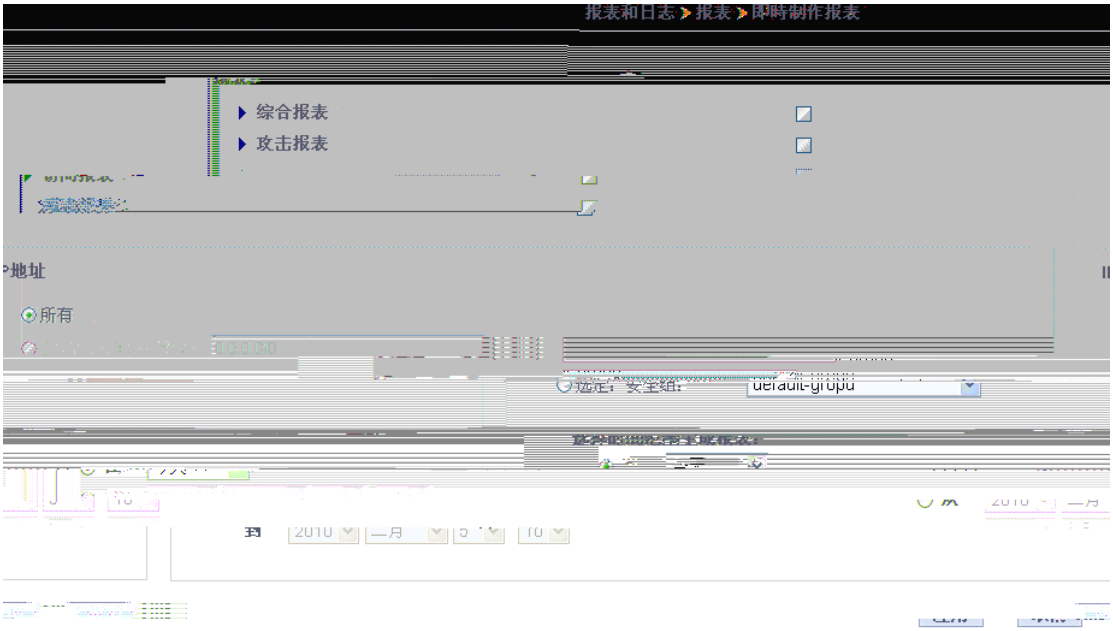
English

6 “ ”

4.1.3

WEBUI

1


报表和日志 > 报表 > 即時制作报表
综合报表
攻击报表
地址
所有
default-group

2 “ ” “ ” “ ” “

” “ ” “ ”

“ ”


客户端攻击事件排名
数目
10

A “ ” “

4.2.1

SQL

WEB

WEB

IP WEB

WEB URL URL POST Cookie

WEB

IP WEB

Cookie

http

1

“ ”

“ ” 25

“ ”

“ ” “

”

2

IP	WEB IP
IP	WEB IP
	WEB GET URL POST

URL URL ㄋ

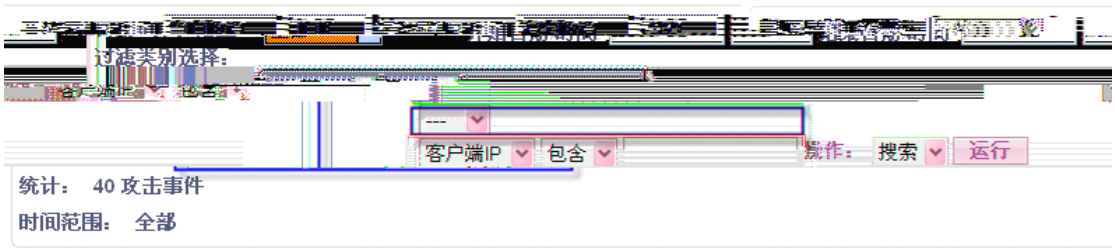
3 “ ”

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

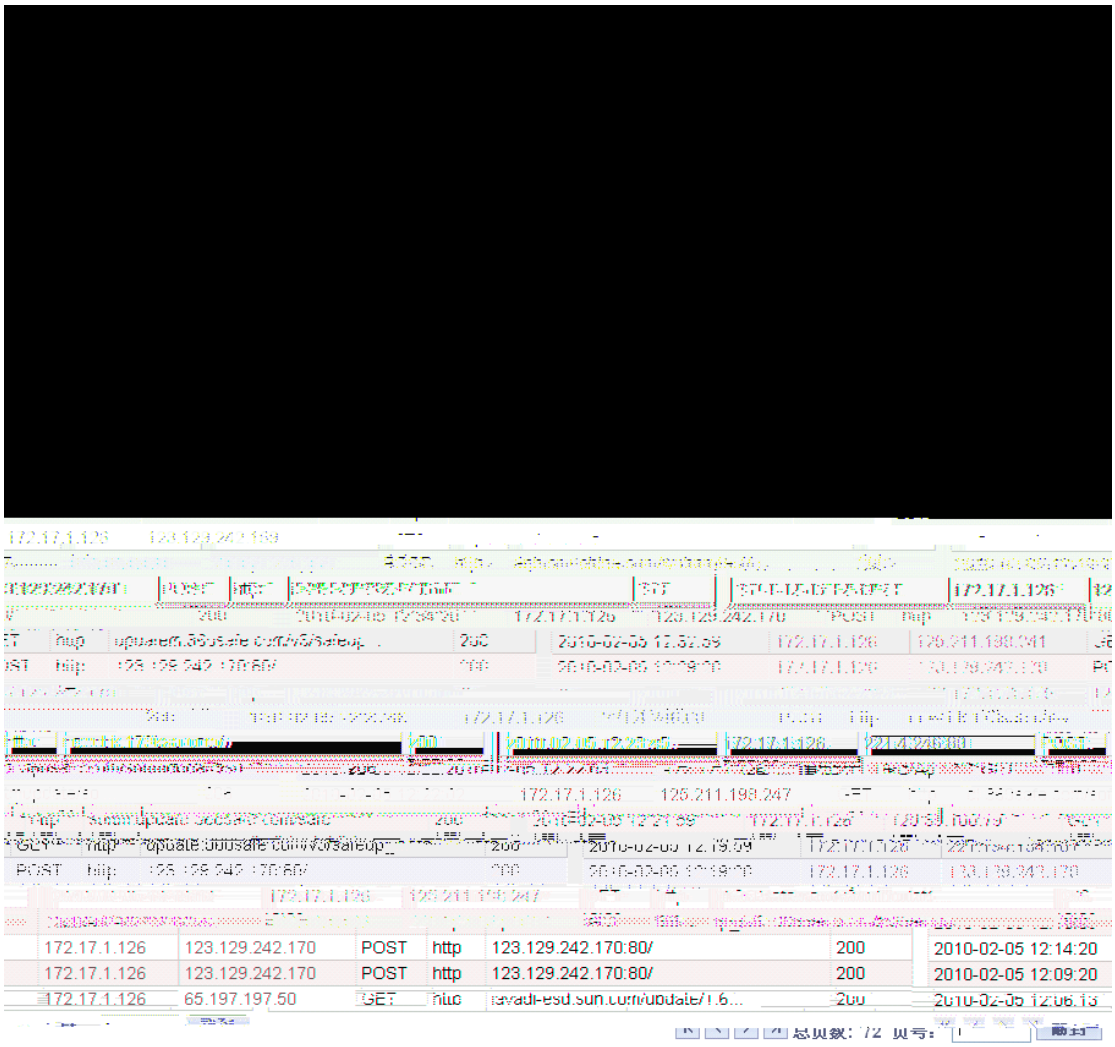
IP WEB IP

URL URL

~ 33 3 ł ` Ф ɀ Ω ƕ ☪ ⊢ ɳ ₽ q '

“ ” “ ”

C “ ” “ ”



“ ”

“ ” 25

“ ”

“ ” “

”

2

	WEB
IP	WEB IP
IP	WEB IP
	WEB GET

3 3 3

“ ” “ ”

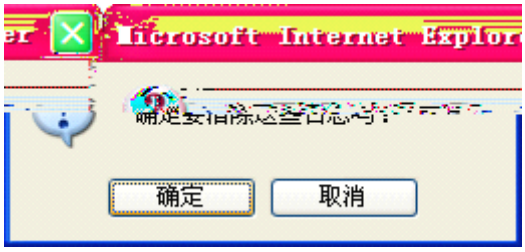
C “ ” “ ”

“ ”

D “ ”

“ ”

“ ”



4.2.4

1


报表和日志 > 日志 > 管理 > 管理员日志
搜索
运行
管理员
包含
操作：
统计： 372 管理事件
时间范围： 全部
日期 时间
来源IP
管理员
动作
administrator logged in from the W
manually update Firmware: update
exec update firmware
set dynamic-blacklist
server group yzf: set anti-overflow
unset client-blacklist entry 172.17.1.130/32
unset client-blacklist entry 172.17.1.125/32
set interface eth1 inbound
set client-blacklist entry 172.17.1.125/32
2009-12-31 10:49:09 192.168.11.131 administrator server group yzf: set anti-overflow max-post-data-length 134
server group yzf: unset trojan-detection
总页数: 15 页号:

“ ”

“ ” 25

“ ”

“ ” “

”

2

IP	IP

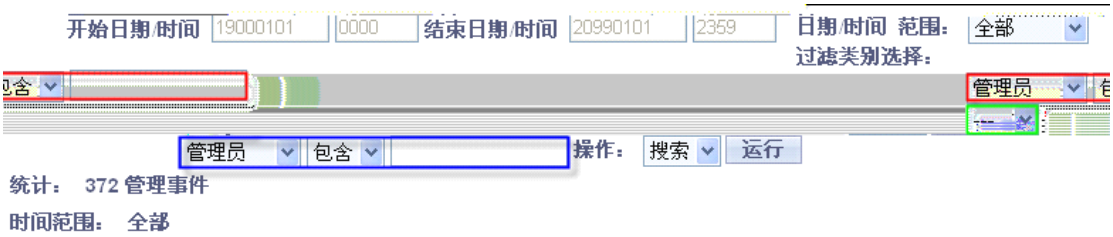
3 “ ”

4 PC “ ”

HTML CSV “ ”

5

IP IP



A “ / ”

“ ” 00:00:00

“ ” 00:00:00

“ 7 ”

“ ” 1 00:00:00

“ 30 ” 30

“ ” “ / ” “ / ”

1

B “ ”

“ ” “

”

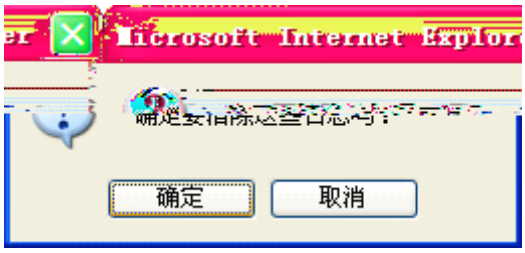
C “ ” “ ”

“ ”

D “ ”

“ ”

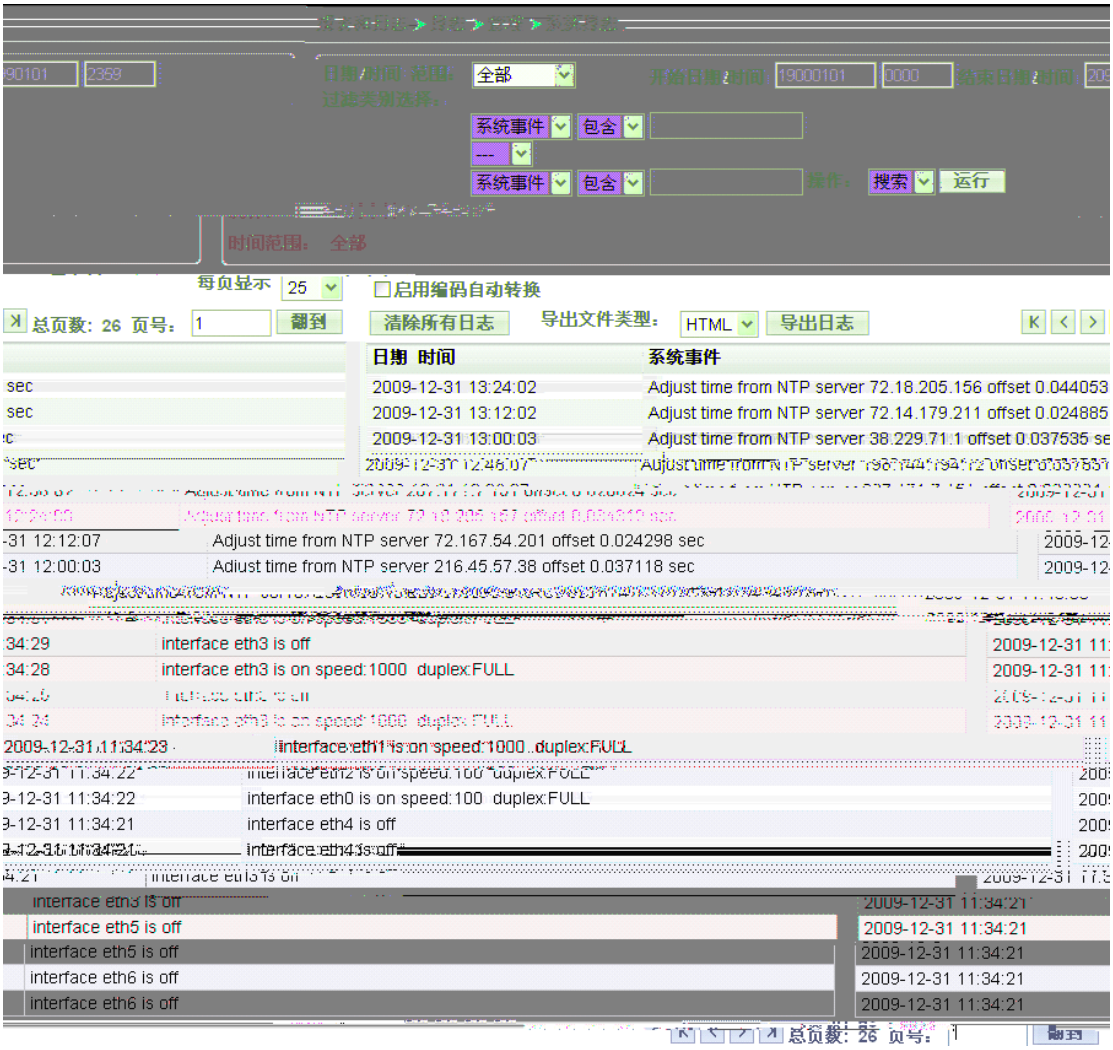
“ ”



4.2.

HA

1


全部
系统事件
包含
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
翻到
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
2009-12-31 13:24:02 Adjust time from NTP server 72.18.205.156 offset 0.044053
2009-12-31 13:12:02 Adjust time from NTP server 72.14.179.211 offset 0.024885
2009-12-31 13:00:03 Adjust time from NTP server 38.229.71.1 offset 0.037535
2009-12-31 12:12:07 Adjust time from NTP server 72.167.54.201 offset 0.024298 sec
2009-12-31 12:00:03 Adiust time from NTP server 216.45.57.38 offset 0.037118 sec
interface eth3 is off
interface eth3 is on speed:1000 duplex:FULL
2009-12-31 11:34:23 interface eth1 is on speed:1000 duplex:FULL
2009-12-31 11:34:22 interface eth0 is on speed:100 duplex:FULL
2009-12-31 11:34:21 interface eth4 is off
interface eth5 is off
interface eth5 is off
interface eth6 is off
interface eth6 is off
2009-12-31 11:34:21
总页数: 26 页号:
翻到

“ ”

“ ” 25

“ ”

“ ” “

”

2

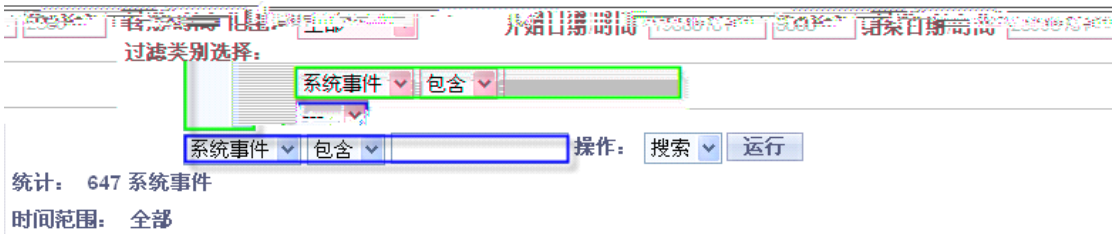
3 “ ”

4 PC “ ”

HTML CSV “ ”

5

IP IP



A “ / ”

“ ” 00:00:00

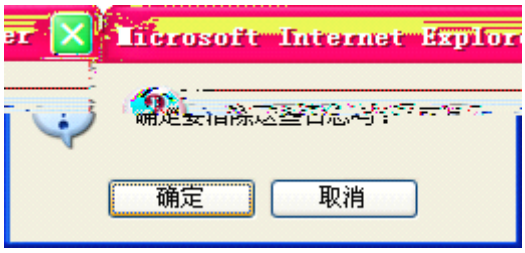
C “ ” “ ”

“ ”

D “ ”

“ ”

“ ”



注释：点击规则名称可对规则属性进行编辑。

1

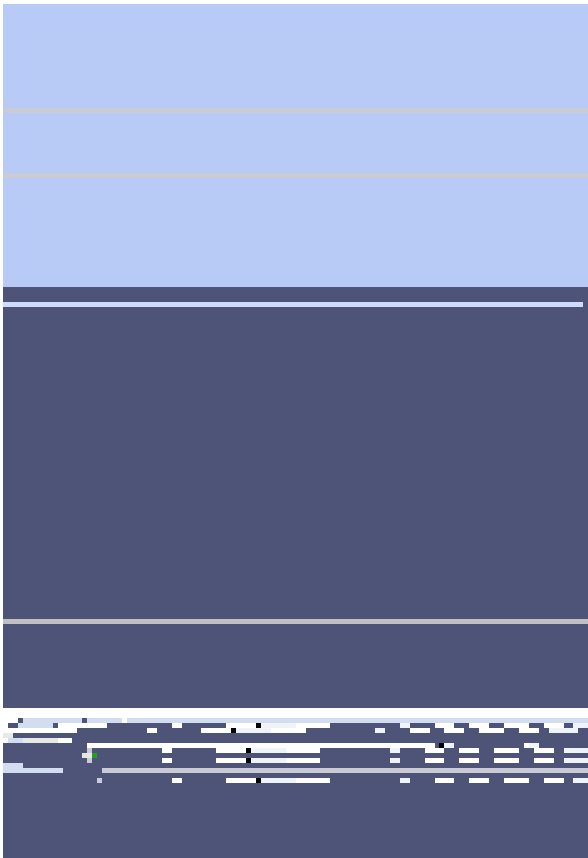
2 “
”

3
“ ”
WEB
SQL WEB SQL
SQL

XSS
WEB
WEB

c “ ” “ ”
“ ”

3



5

“ ” “ ”

.1.1

SQL WEB SQL

(POST GET)

RG-WG

SQL SQL SQL

1 “ ” SQL

“ ”

2 “ SQL ” WEB SQL

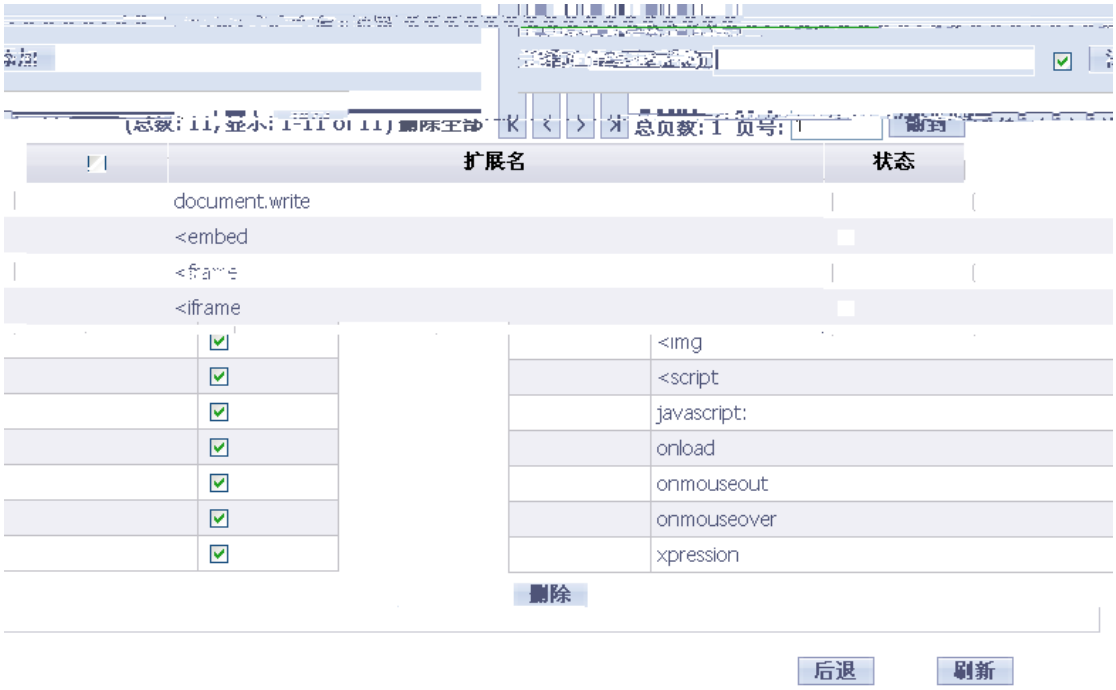
“ ”

3 “ ” SQL

A Web B

CGI

HTML

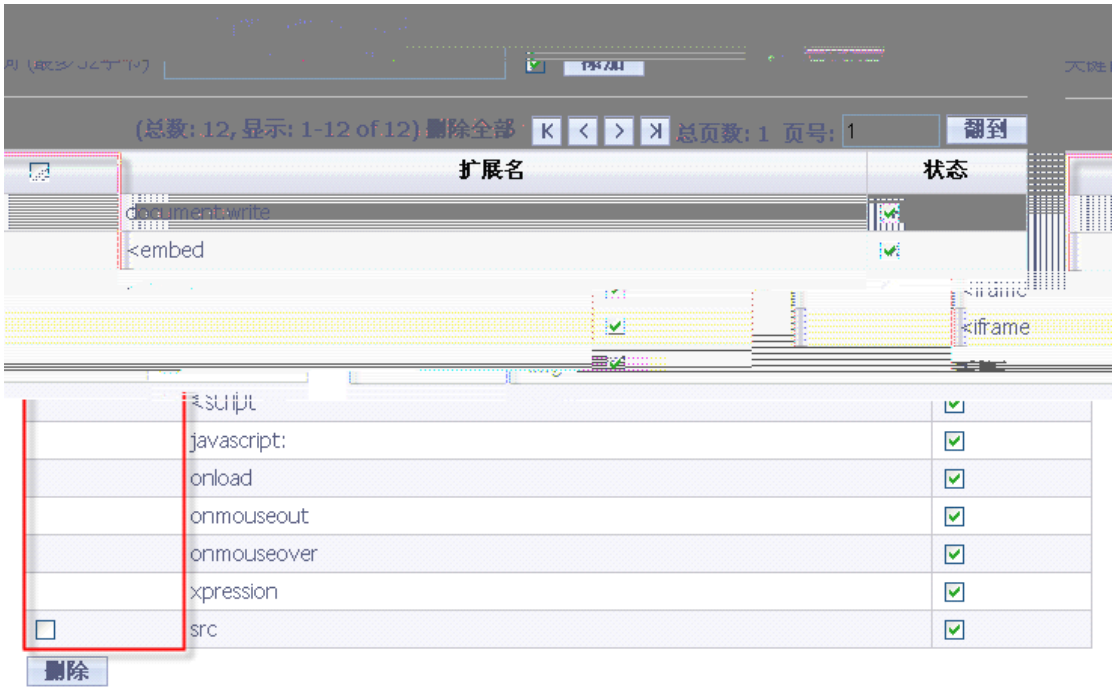

扩展名
状态
document.write
<embed
<iframe
<img
<script
javascript:
onload
onmouseout
onmouseover
xpression
删除
后退
刷新

“ ”

A

“ ”

“ ”


(总数: 12, 显示: 1-12 of 12) 删除全部
总页数: 1 页号: 1
翻到
扩展名
状态
<embed
<iframe
javascript:
onload
onmouseout
onmouseover
xpression
src
删除

B

“ ”

.1.3

HTML

( )

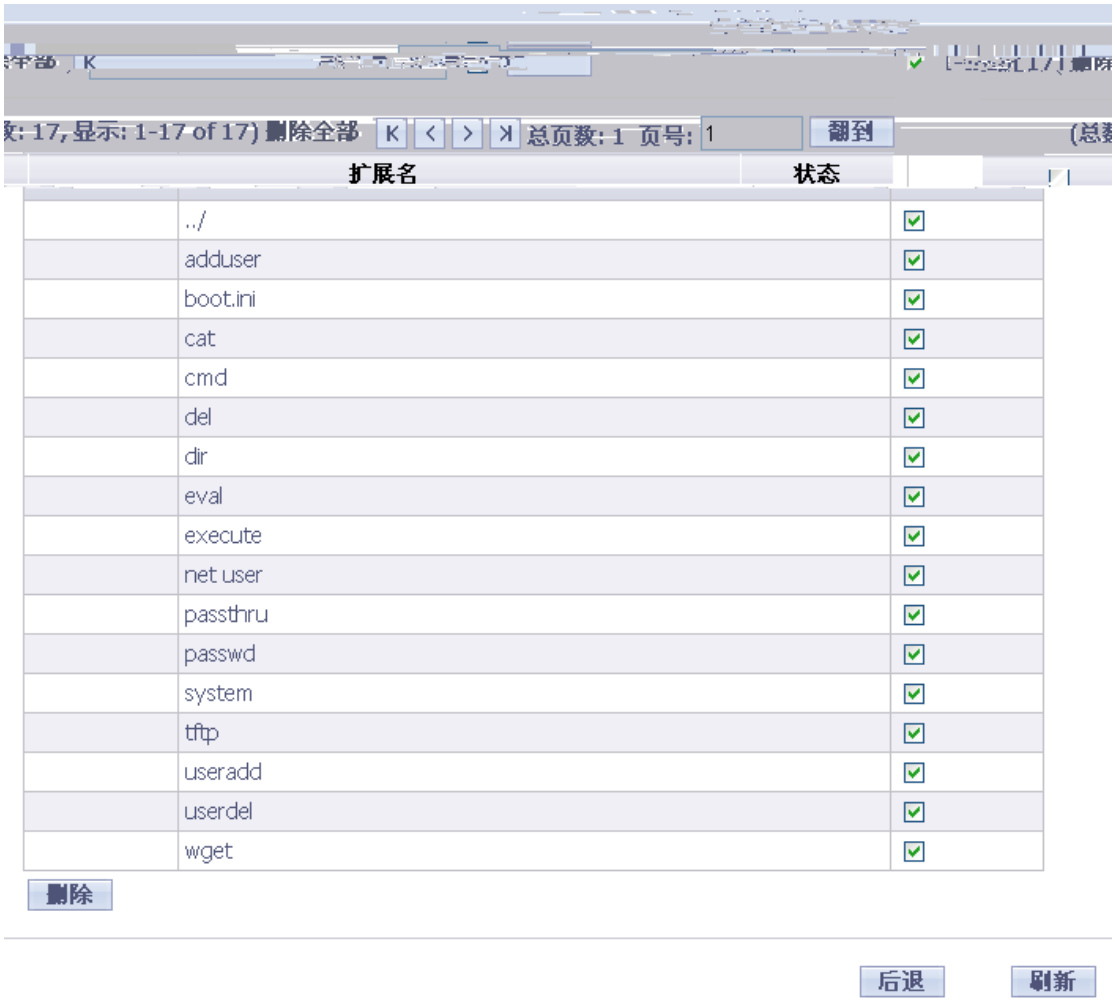
RG-WG

1 “ ”

“ ”

2 “ ”

3 “ ”


: 17, 显示: 1-17 of 17) 删除全部
总页数: 1 页号: 1
翻到
扩展名
状态
../
adduser
boot.ini
cat
cmd
del
dir
eval
execute
net user
passthru
passwd
system
tftp
useradd
userdel
wget
删除
后退
刷新

“ ” “ ”

“

4 , 150 password,

00000,8888

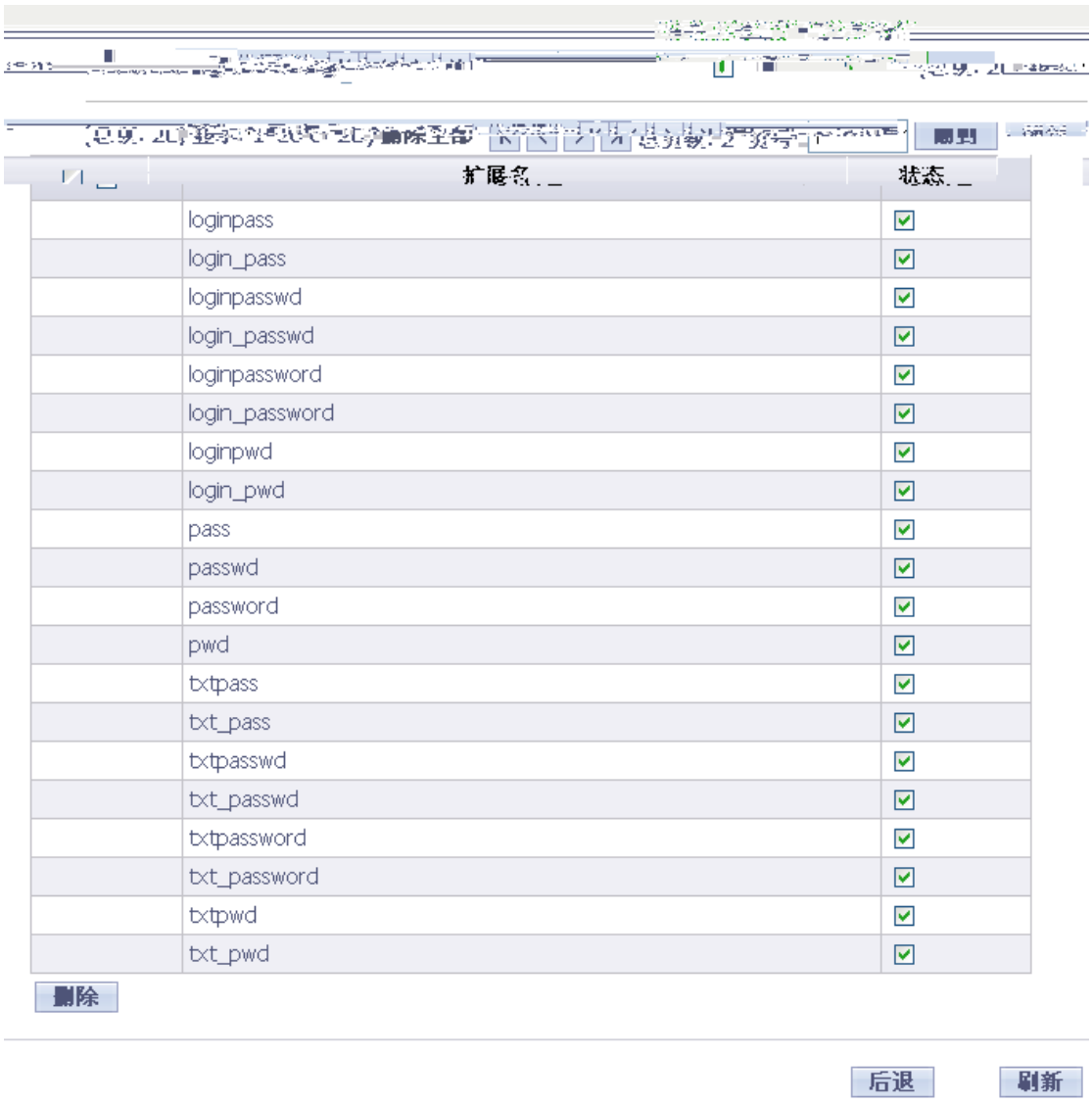
RG-WG WEB

“ ”

RG-WG

WEB

- 2.0 4


扩展名
状态
loginpass
login_pass
loginpasswd
login_passwd
loginpassword
login_password
loginpwd
login_pwd
pass
passwd
password
pwd
txtpass
txt_pass
txtpasswd
txt_passwd
txtpassword
txt_password
txtpwd
txt_pwd
删除
后退
刷新

“ ” “ ”

“ ”

.1.

WEB

RG-WG WEB

“

.1.

WEB RG-WG WEB

“ WEB ” RG-WG WEB

“ ” “ ”

“ ” “ ” “ ”

“

”

.1.

RG-WG

WEB

1 “ ” RG-WG “

” WEB “ ”

“ ” “ ” “ ”

“ ”

“ ”

2

“ mdb ”

WEB RG-WG “ mdb ”

WEB

A

“ ” “ ”

B “ ”

3

C “ ” “ ”

RG-WG

.1.

RG-WG WEB

WEB

1 “ ” RG-WG “

” WEB “ ”

“ ” “ ” “ ”

“

WEB

WEB

WEB

A

“ ” “ ”

B “ ”

C “ ” “ ”

RG-WG

.1.10

“ IP ” WEB RG-WG

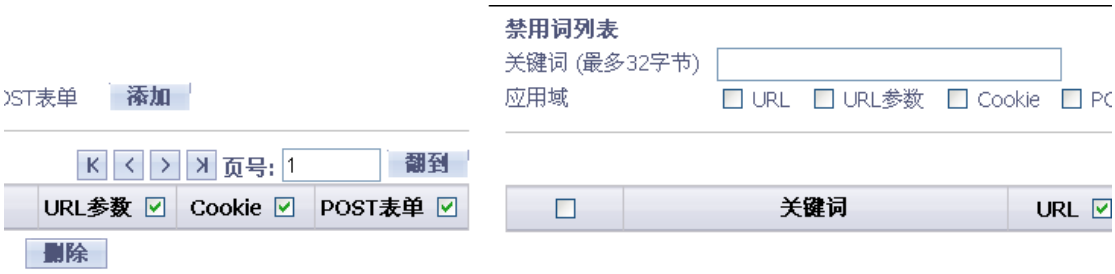
“ IP ” IP

IP IP

A IP

“ IP ” IP “ ”

“ ”

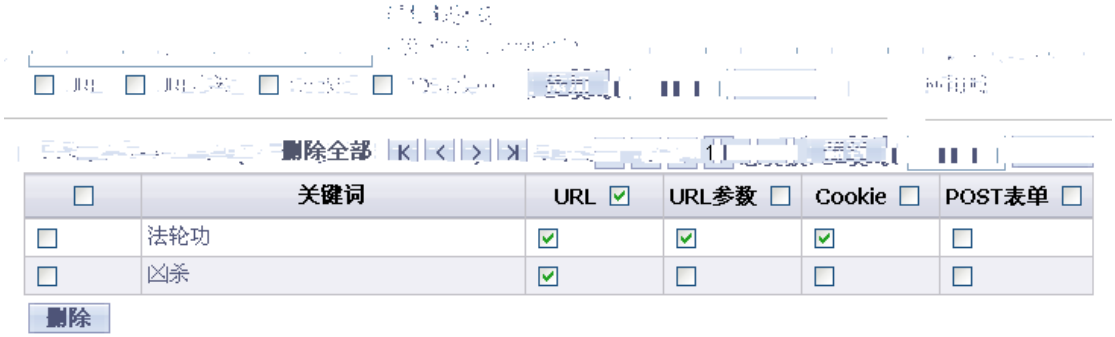


A

“ ” “ ”

“ URL ” “ URL ” “ POST ” “ Cookie ”

“ ”



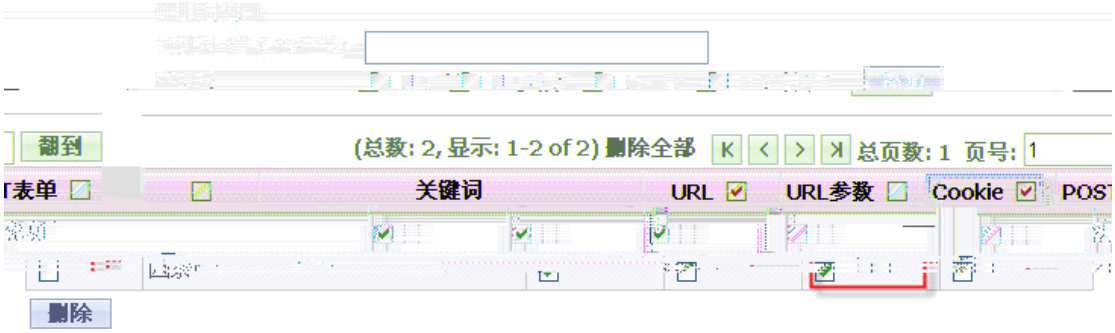
B

“ ”

C

“ ”

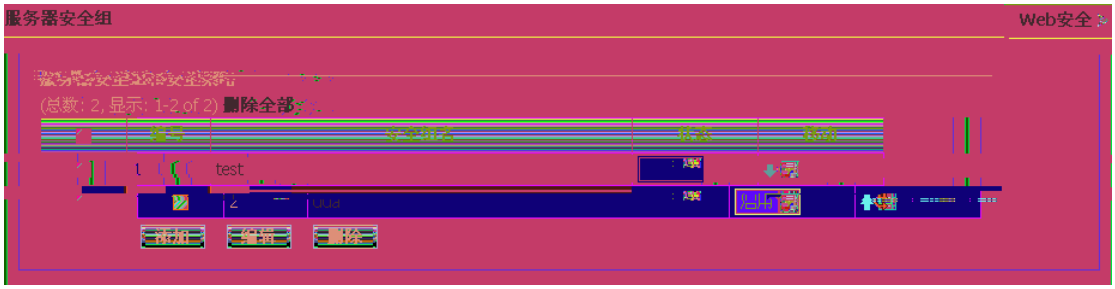
“ Cookie ” Cookie



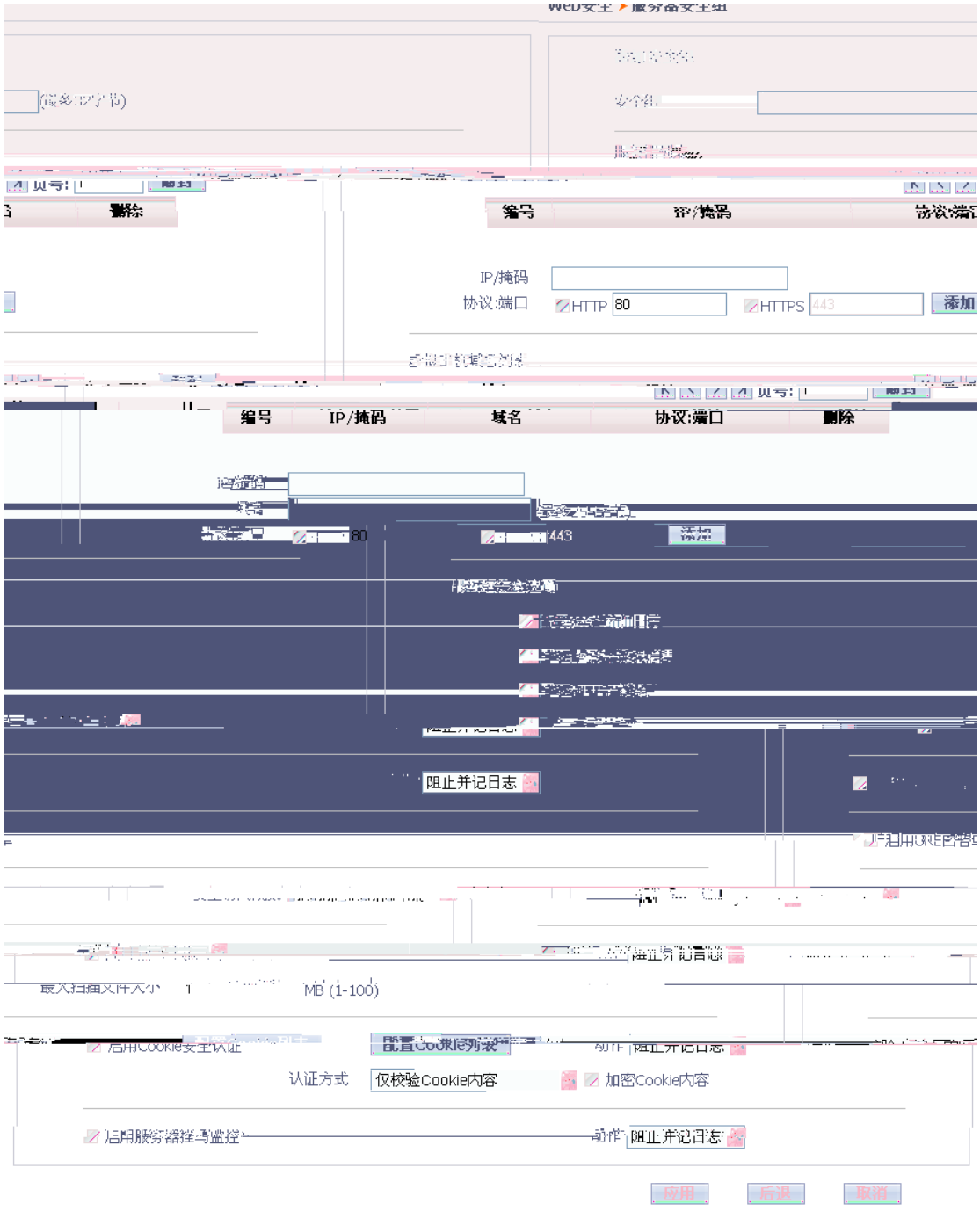
.2

WEB

1



“ ”



A “ ” “ ” “

” WEB IP

WEB

B “ ” WEB

WEB HTTP

“ ” “ ”


Web安全 > 服务器安全组
编辑安全组
安全组 default-group
服务器列表
协议:端口
删除
编号
IP/掩码
HTTP
HTTPS
443
添加
虚拟主机域名列表
翻到
编号
IP/掩码
域名
协议:端口
删除
1
172.17.1.130/32
130.yzf.com
HTTP:80 HTTPS:443
协议:端口
HTTP
80
HTTPS
443
添加
服务器安全选项
记录Web访问日志
屏蔽服务器版本信息
屏蔽HTTP错误码
启用防溢出检查
配置
动作
仅记日志
启用URL黑名单
配置
动作
阻止并记日志
启用URL白名单
配置
安全访问规则
222
配置例外
动作
仅记日志
启用上传病毒扫描
MB (1-100)
最大扫描文件大小
99
认证方式
校验Cookie内容和客户端IP
加密Cookie内容
应用
后退
取消

“ ”

3

“ ” “ ” “

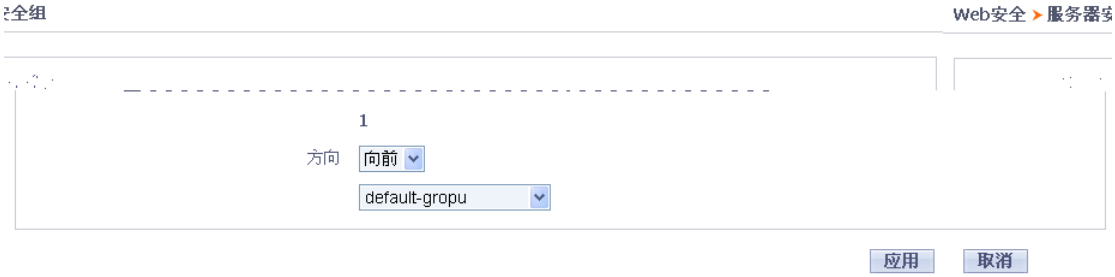
” “ ” “ ” “ ”

4


Web安全 ➤ 服务器安全组
总页数: 2 页号: 1
翻到
状态
移动
服务器安全组和安全策略
(总数: 42, 显示: 1-25 of 42) 删除全部
编号
default-gropu
23 21 启用
24 22 启用
25 23 启用
添加
编辑
删除

“ ”

“ ”


Web安全 ➤ 服务器
1
方向
向前
default-gropu
应用
取消

“ ” “ ” “ ”

“ ”

“ 1 ” “ default-gropu ”

.2.1

WEB

1 “ ” WEB IP

“ IP/ ” WEB IP WEB

“ ”

“ ”

2 WEB “ ”

WEB IP

“ IP/ ” WEB IP “ ” WEB

“ ” WEB

“ ”

“

“ ”

“ ”

HTTP

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

	200 0-200
Cookie	WEB cookie 4096 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 “ ”

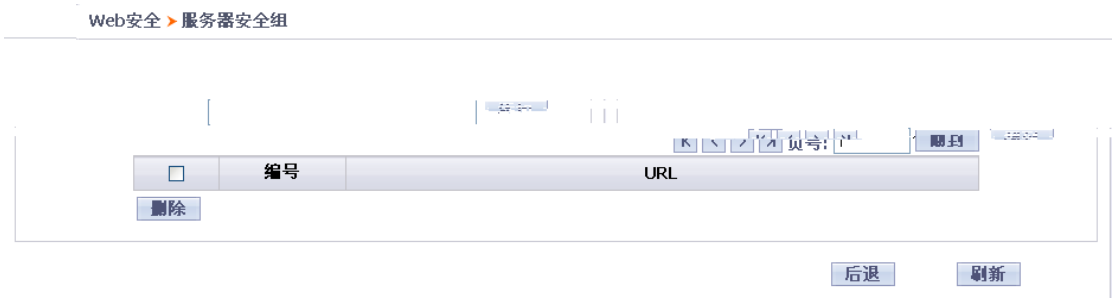
www.sina.com URL

“ ”

WEB WEB URL URL URL URL URL URL

A “ ” URL

B “ ” URL URL URL URL



“ URL ” WEB URL path level URL “ ”

www.sina.com URL

“ ”

.2.4

Web

URL

5.1

1 WEB

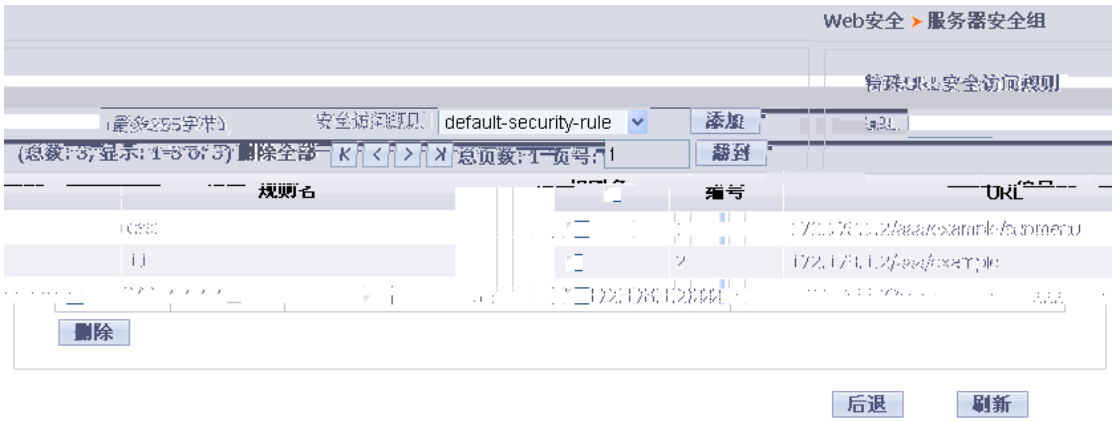
2

URL “ ”

A

“ URL ” URL “ ”

“ ” “ ”



B

“ ”

.2.

RG-WG WEB

1 “ ” “ ” RG-WG WEB “ ”

1 WEB

2 WEB

3 WEB

2

100 M

WEB Cookie

IP Cookie Cookie

Cookie “ ” “ Cookie

” “ Cookie IP ”

Cookie

1 Cookie

2 Cookie IP

Cookie Cookie RG-WG

cookie list cookie

.2.

RG-WG WEB WEB

1 “ ”

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

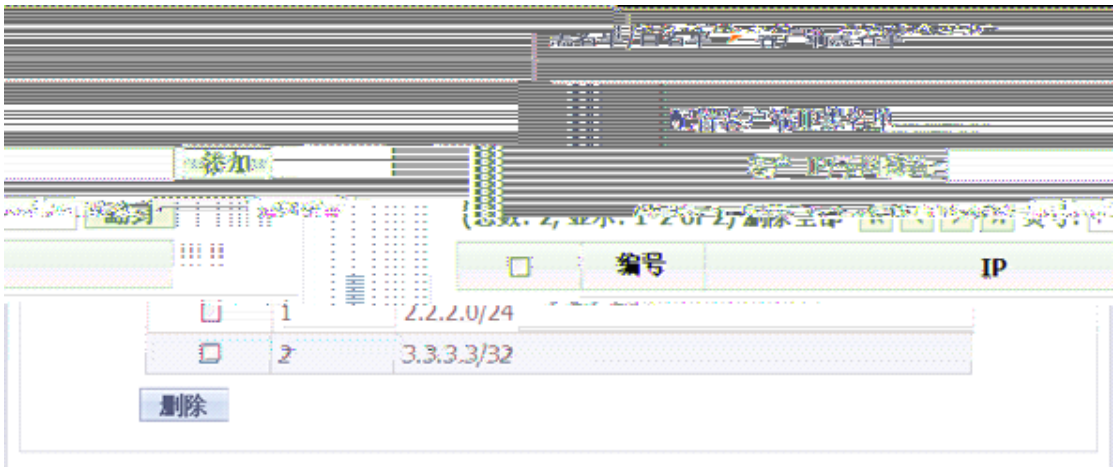
7 “ ” URL

8 “ ” IP

.1

IP WEB

1 /



2

“ IP ” IP “ "

3

“ ”

.2

Ruijie RG-WG IP WEB

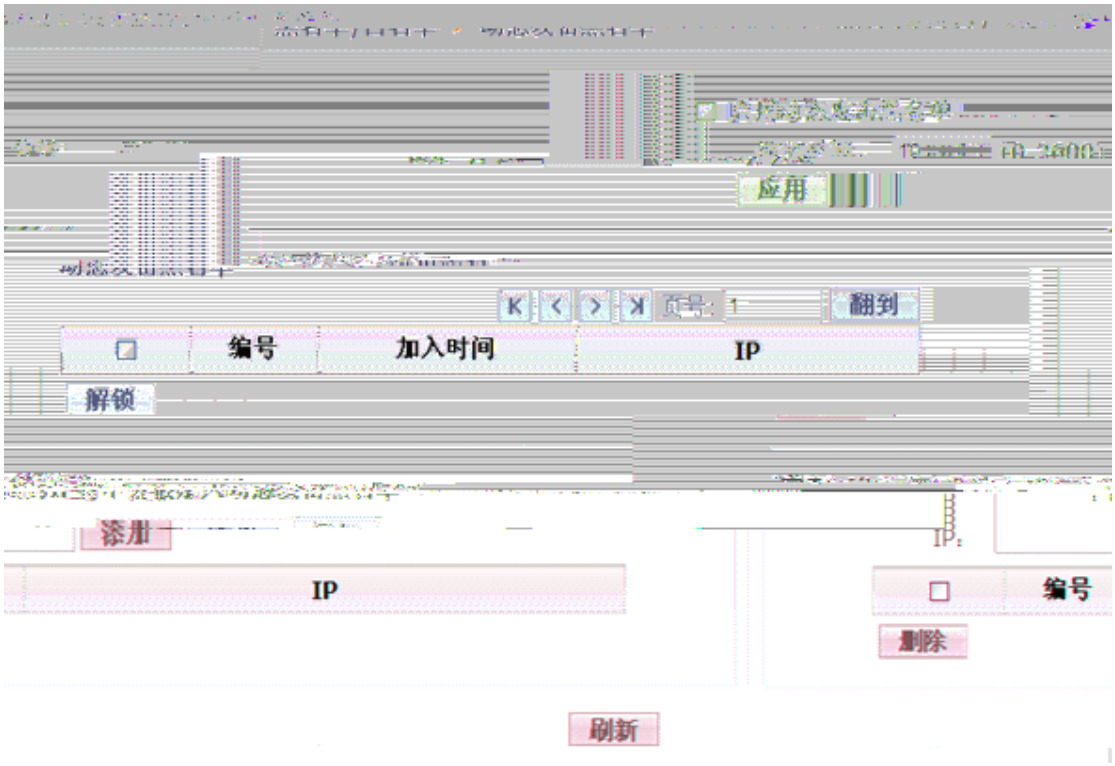
SQL “ block " RG-WG

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

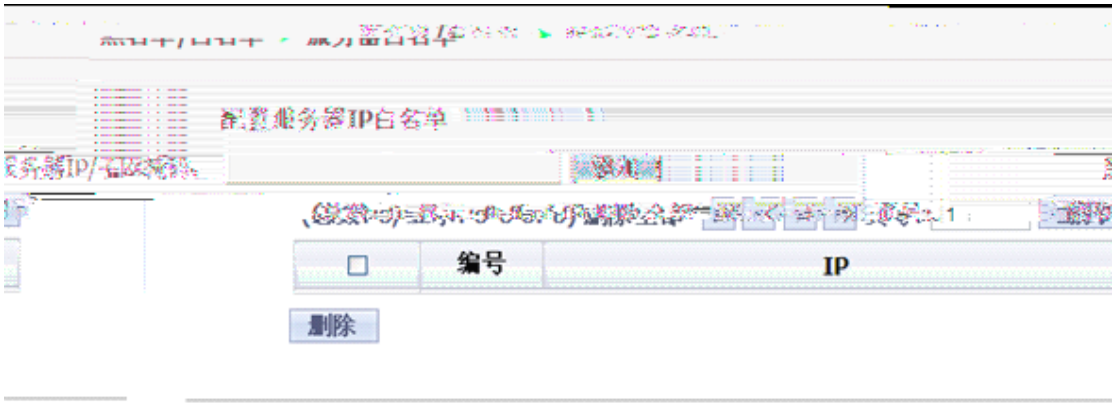
1 /

2

“ IP ” IP “ ”

3

ㄋ ㄋ



2

“ IP/ ” IP

“ ”

IP “ ”

“ ”

3

“ ”

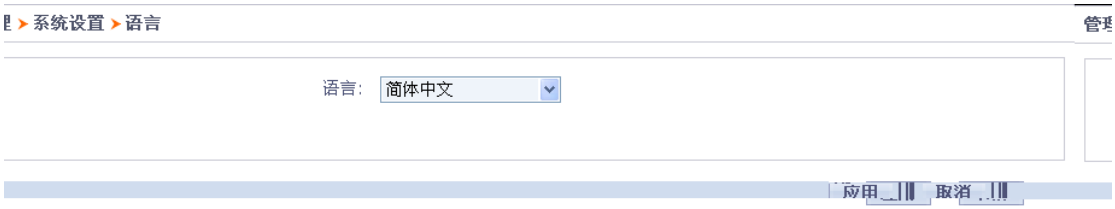
.1

.1.1

RG-WG WEBUI

. 1

1



2 “ ”

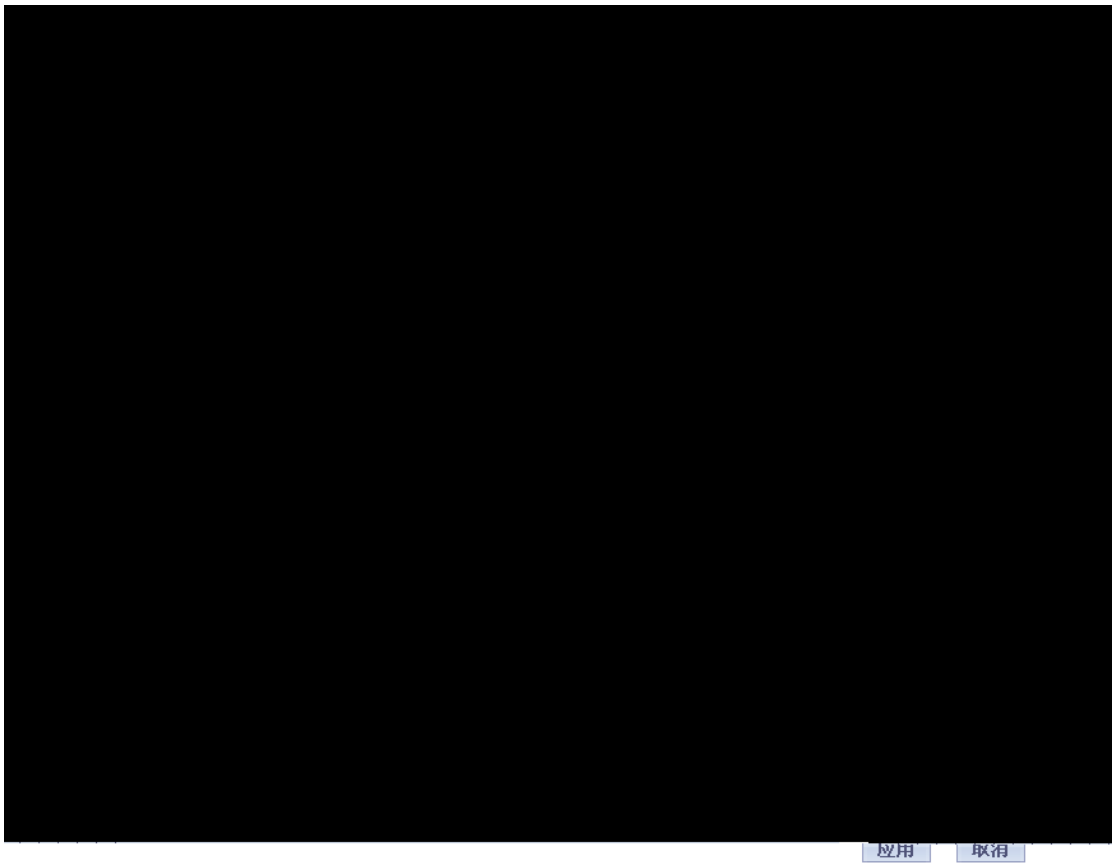
3 “ ”

.1.2

SNMP SNMP

NTP

DNS



.1.2.1

“ ”

“ ”

‘ _ ’

“ ”

.1.2.2

SNMP polling SNMP

1 “ SNMP ”

2 “ Community ” SNMP SNMP

SNMP

3 SNMP

“ ” WEBUI “ ”

1

“ ”

2 NTP

“ NTP ”

NTP

NTP

“ ” NTP

“ ”

首选DNS服务器 202.106.196.115

备选DNS服务器

“ ”

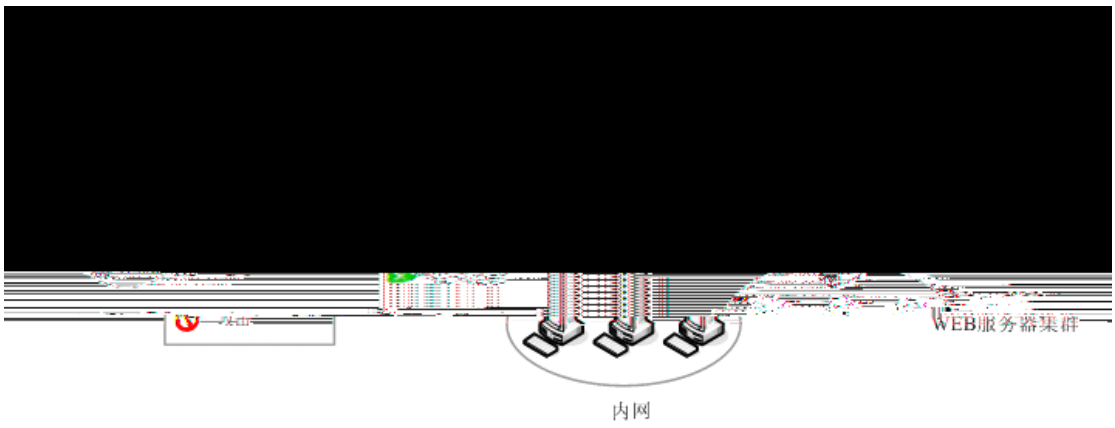
.1.3

.1.3.1

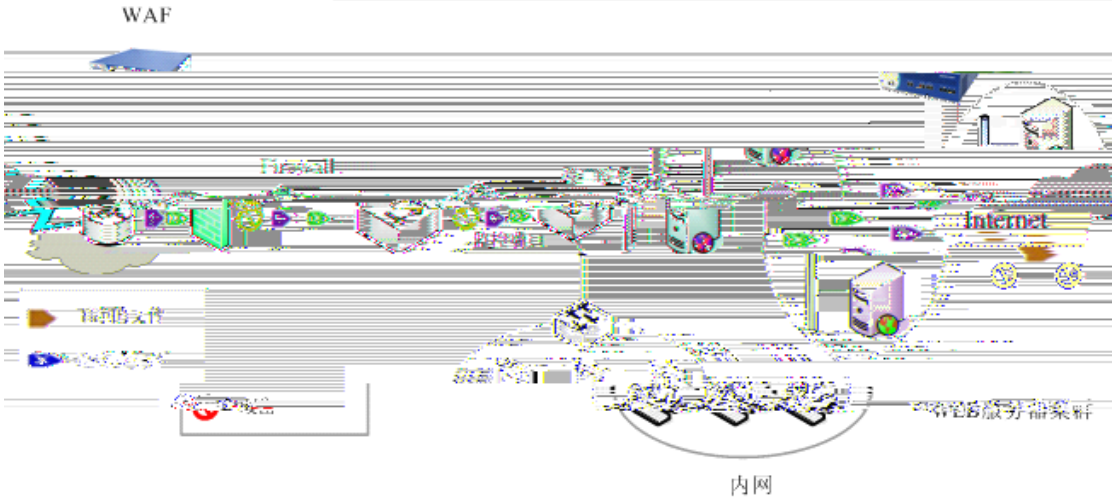
WEB WEB

HTTP/HTTPS WEB

WEB WEB



SPAN



span

WEB

WEB

1

2

3 “ ”

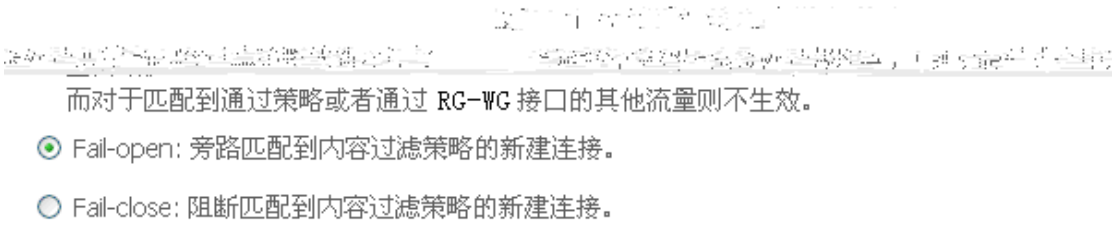
4

.1.3.2

RG-WG bypass failopen

WEB

1



2

Fail-open WEB

Fail-close WEB

3 “ ”

.1.3.3

Ruijie RG-WG HTTP/HTTPS

“ ”

Ruijie

WEB

1

2 “ ”

3 “ ”

.1.3.4

TCP TCP

TCP

1

2 “ TCP ”

3 “ ”

.1.4

WEB

HA QMAIL

1


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
应用
取消

2

“ ”

.1.

1

2 “ ” 1-60

3 “ ” 1-1000 (MB)

4 “ ”

.1.

FTP Syslog

.1. .1

FTP

1

FTP

2

	5000-50000 MB
	1 - 100
	1 4.2.4 2 HA 4.2.5 3 WEB WEB

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 ┍

HA

WEB WEB

Syslog

3 Syslog

IP Syslog IP

Syslog

Syslog “ ” Syslog

“ ” “ ” “ ” “ ”

syslog

7 0

7

4 “ ”

.1.

RG-WG SNMP Trap HA

“ ” 7.1.4

.1. .1

RG-WG HA HA

“ ”

WEB

1

2 HA “ HA ”

3 “ ”

4 “ ”

.1. .2

SNMP trap SNMP

SNMP

SNMP v1 v2 SNMP 7.1.2.2

SNMP

SNMP SNMP trap SNMP

1

RG-WG

IP

IP

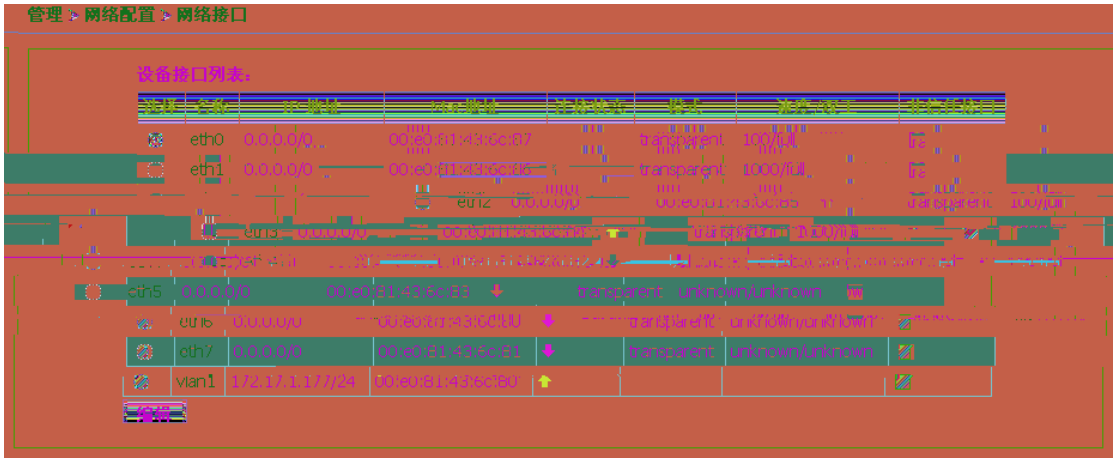
.2.1.1

RG-WG

.

RG-WG

RG-WG



VLAN

.2.1.3

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 I D

Trunk “ 802.1Q VLAN ” VLAN ID

ID “ ” “ ”

VLAN ID VLAN ID

VLAN ID “ ” “ ”

VLAN ID VLAN ID

1

VLAN 1 VLAN 1

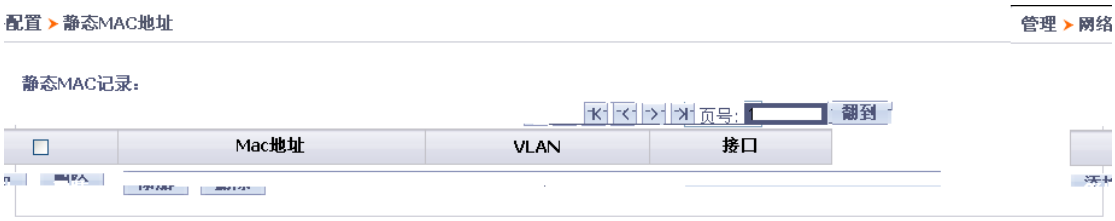
“ Native VLAN ” “ ”

.2.3

MAC

MAC

1



2

MAC	MAC
VLAN	MAC VLAN
	MAC

3 “ ”

ARP IP ARP

ARP Ruijie

1

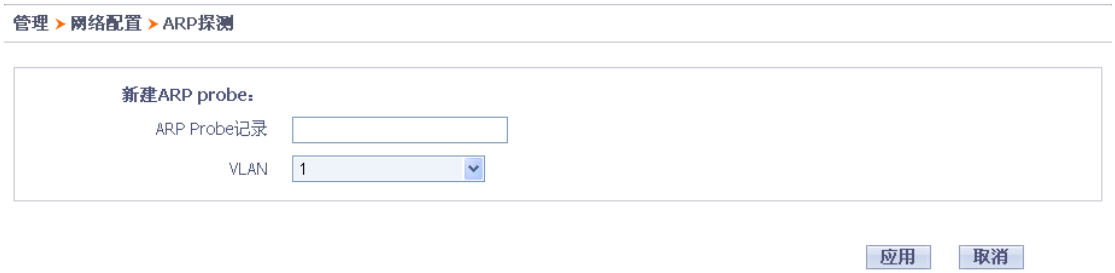
2 ARP

“ IP ” IP

“ VLAN ” IP VLAN

3 ARP

“ ”



“ ARP Probe ” IP IP

ICMP

1

“ ” “ ”

0.0.0.0

2

A “ ”

“ ”

“ ” 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 “


管理 ➤ 网络配置 ➤ 高可用性
ster
设置Failover
启用HA
HA状态 Ma
Failover状态 No
MAC Block
.0.0/0
集群IP地址/掩码 0.0
HA接口
(1-254) 设置254将成为主机
HA优先级 100
(1-254) 1为默认值
组ID 1
(1-30) 秒
保持间隔 1
.0.0
对等IP 0.0
启用设备故障切换临界值
(1-32)
3
32
eth0
eth1
eth2
eth3
eth4
eth5
eth6
eth7
(0-600) 秒
应用
取消

22 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 ”

“ ”

“ ”

A “ ”

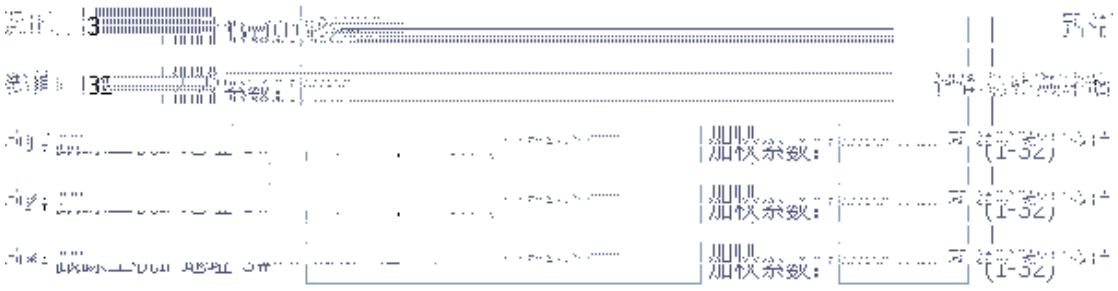
B “ ” HA

1-32

VRRP

UP

Master



A “ ”

ping

3

B “ ”

“

” VRRP

23 1 12 2 15 1

2 23 “ ” “ ”

11 1 2

C “ IP ” IP

ping

D “ ` ך ל n ל

Master

0 600 “ 0 ”

“ ”

.2. .3

HA pair

WEBUI IP

HA CLI WEBUI

` ㇀ ~ n `

Ruijie RG-WG HA HA IP

.2. .

HA pair

HA

1 vlan1 IP

7.3.1.1

2

“ Failover ”

CLI #set ha failover

3

7.3.1.1

4 “

Failover ”

.3

.3.1

.3.1.1

RG-WG

4

3

“

b “ ” “ ” “ WEB

” “ ”

5

a

b “ ” “ ” “ WEB

” “ ” “ ”

6

“ ” “ WEB ”

“ ” “ ” “ ”

Web “ ” 1042.11

1000.41 “ " 1042.11

“ WEB ” RG-WG

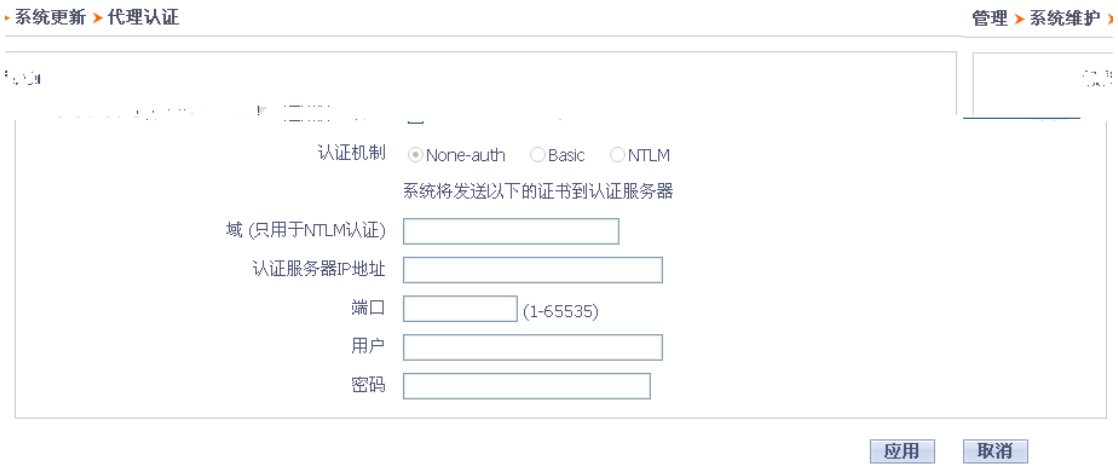
1000.41

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



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

2 “ ”

.3.2

WEB RG-WG

WEB

“ ”

License

WG License

License License

License

1

2

“ ” “ ”

.3.3

WEBUI RG-WG

1

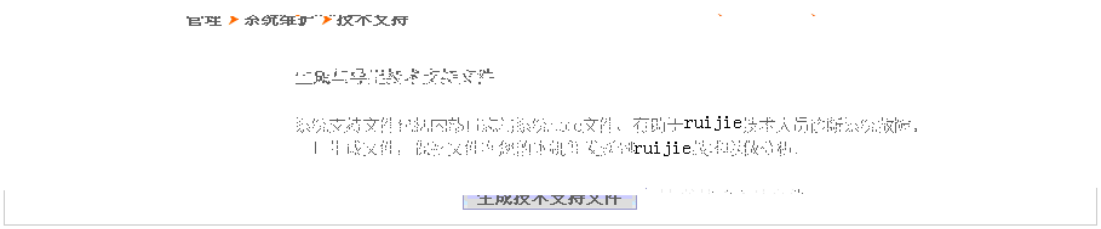
2 “ ”

3 “ ”

.3.4

“ ”

1



2 “ ”

3 PC

.4

RG-WG

administrator

administrator WEB CLI

.4.1

WEBUI CLI RG-WG

——

——

——

“ administrator ”

“ administrator ” 9

1

2

“ ”

	“ ”
	Read-write ——

	Read-only —— Audit ——

3 “ ”

.4.2

HTTPS SSH

1

	WEBUI 5-30 15
	0- 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