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

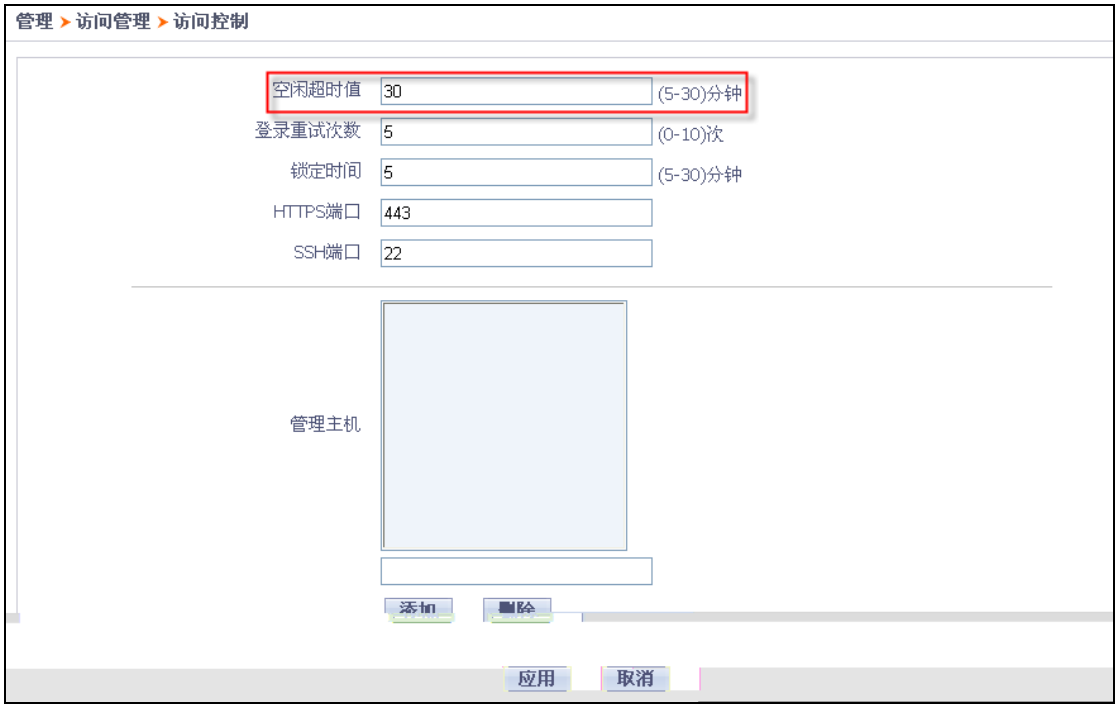
2.2 WEBUI

WEBUI >

WEBUI

-
-
- WEB URL “ ” URL
  WEB
  DoS Webshell

4.A.5.02ETBT1 0 0 1 505.42 72


管理 ➤ 访问管理 ➤ 访问控制
空闲超时值
30
(5-30)分钟
登录重试次数
5
(0-10)次
锁定时间
5
(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

	“ ”
CPU	CPU

“ ”

3.2

>

HTTP

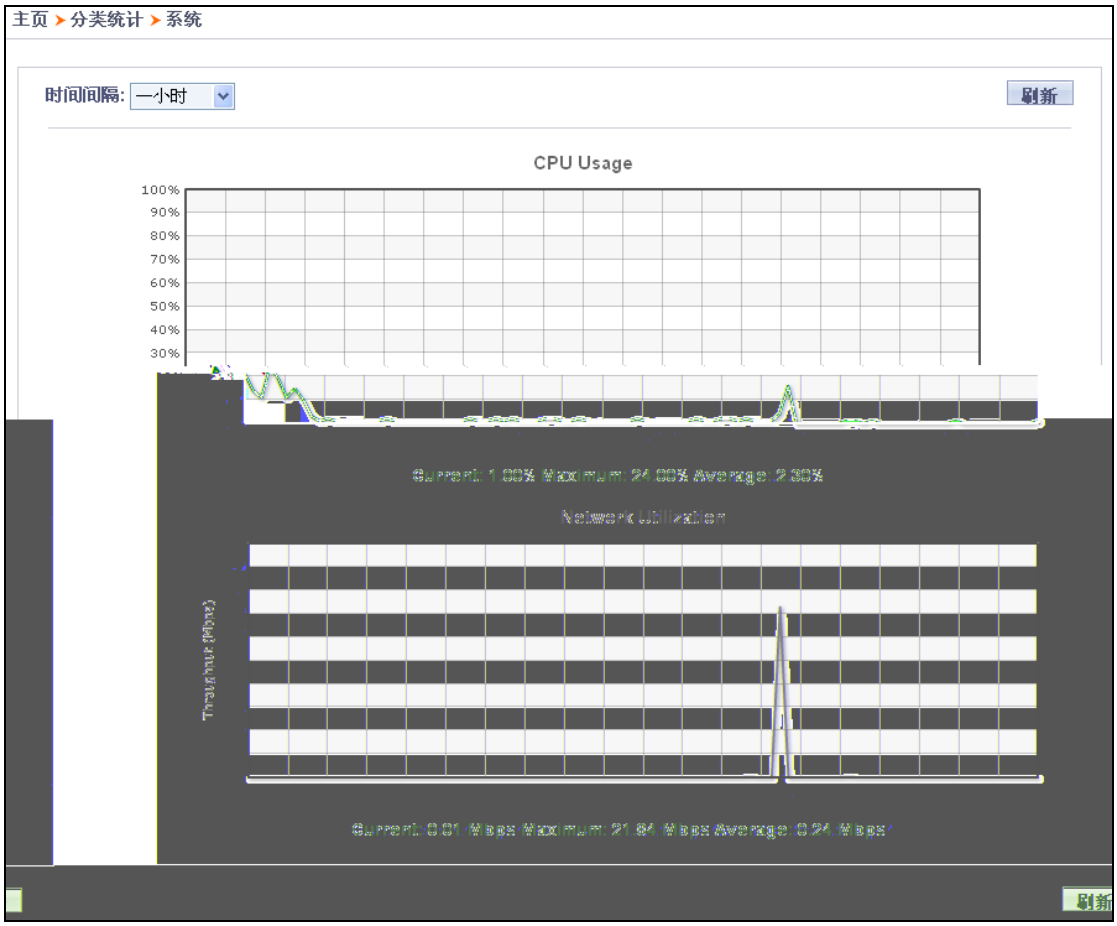
HTTPS

Web

WEB

3.2.1

> > CPU



“ CPU ” CPU

CPU

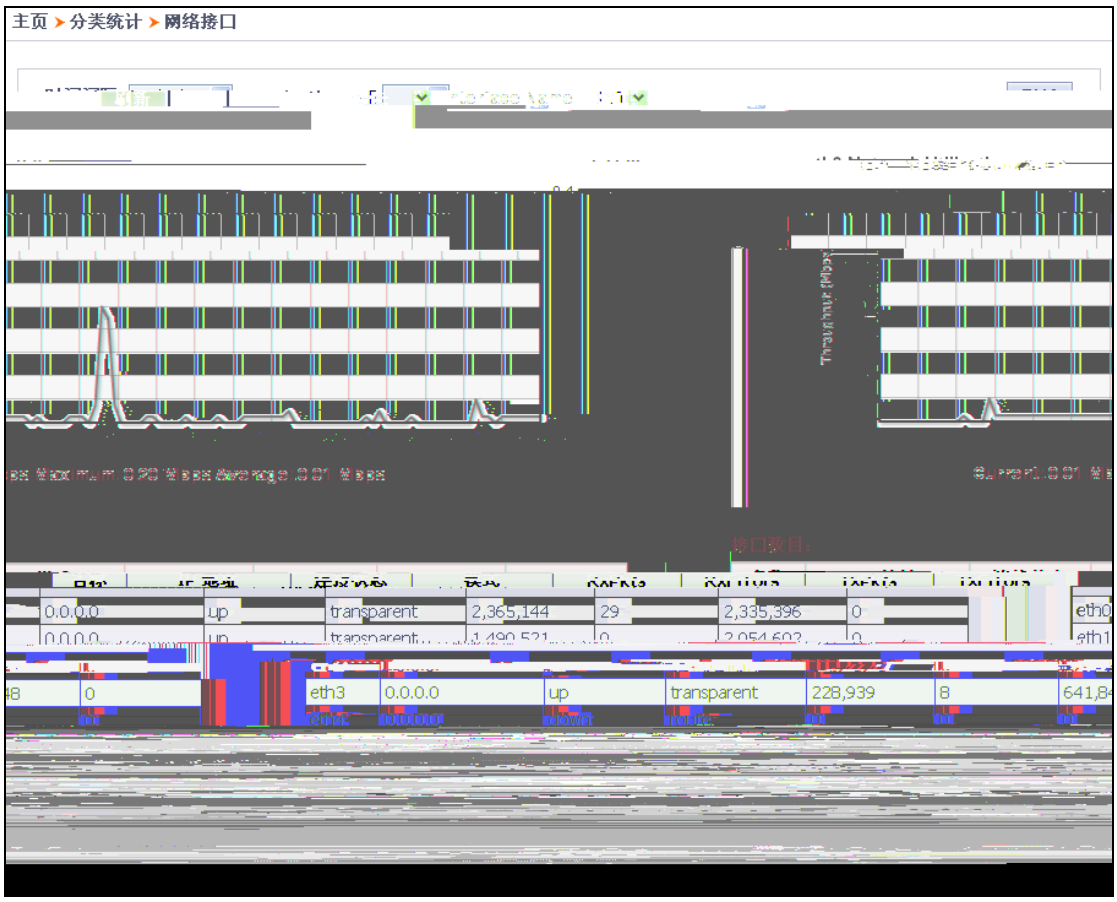
“ ”

“ ”

“ ”

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

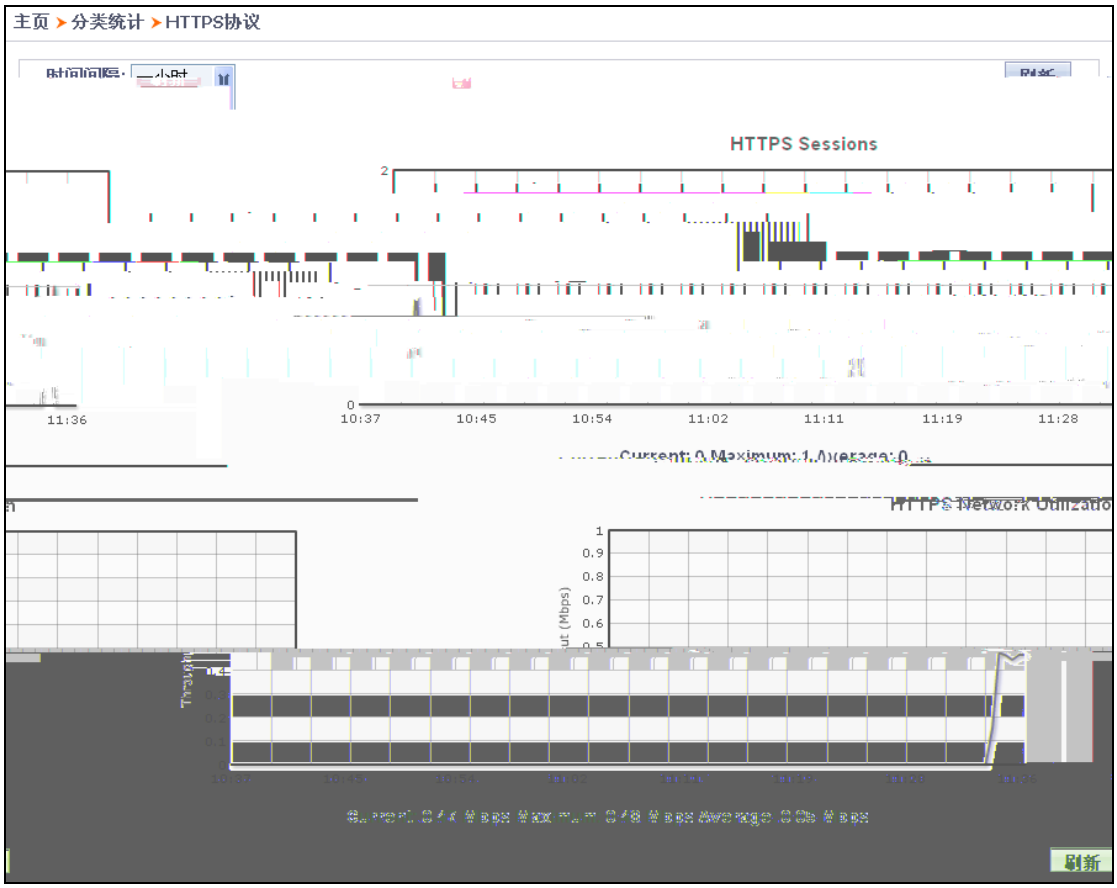
“ ”

“ ”

3.2.4 HTTPS

> > **HTTPS** 1

HTTPS



“ ”

00 01

00 01

7

1 00 01

30 30

“ ”

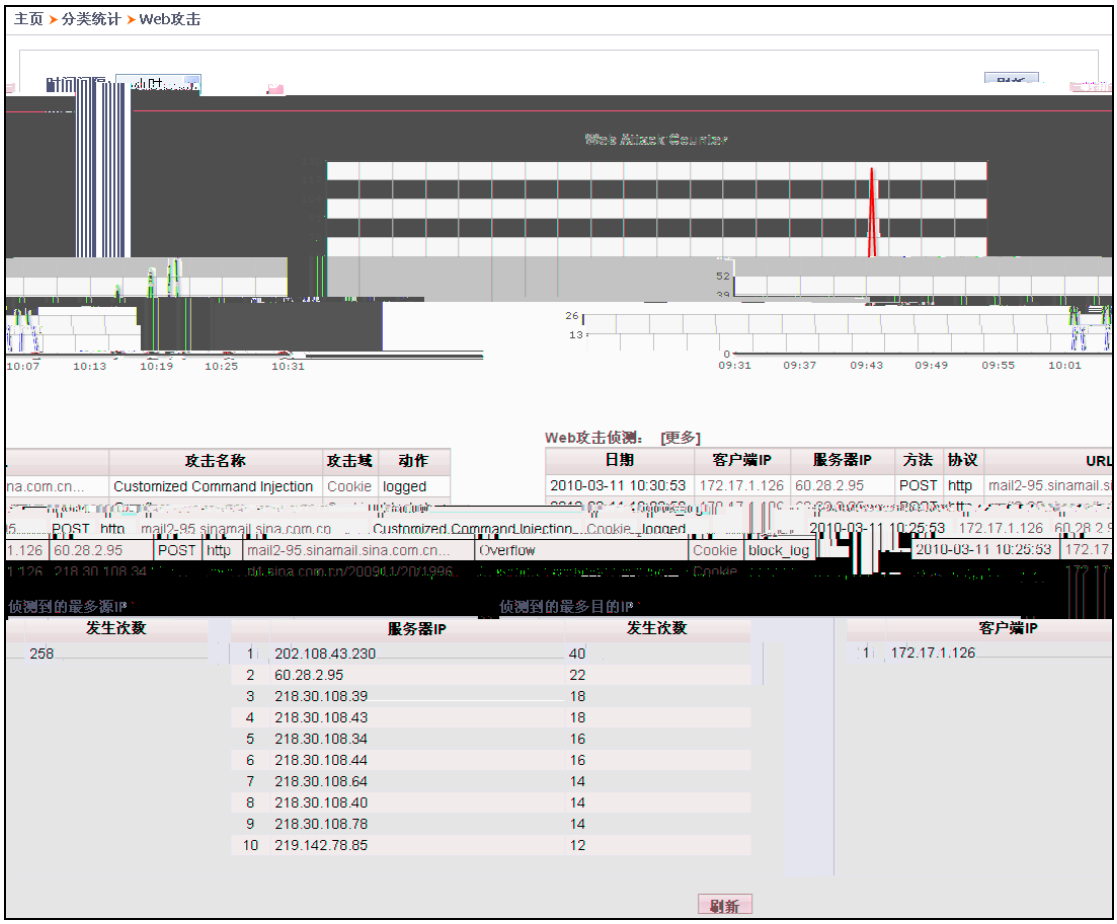
“ ”

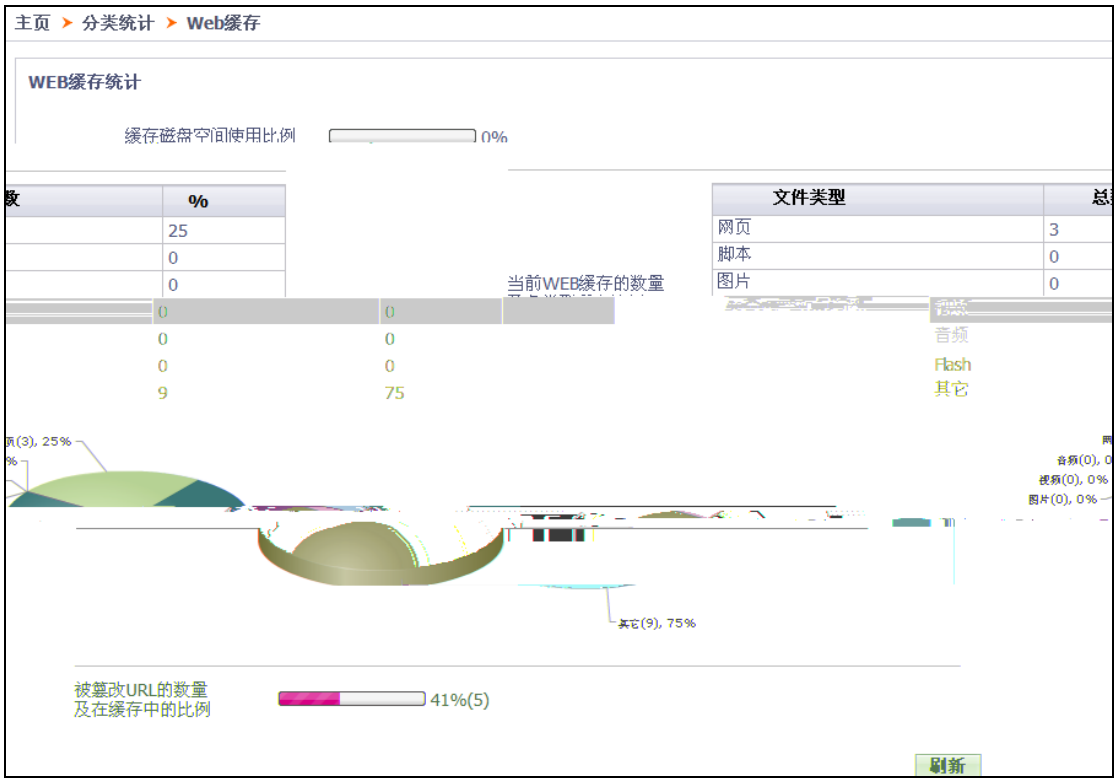
3.2.5 WEB

WEB

WEB WEB

> > **WEB** WEB





“ ”

“ WEB ”

4

WEB

WEB

WEB

4.1

RG-WG

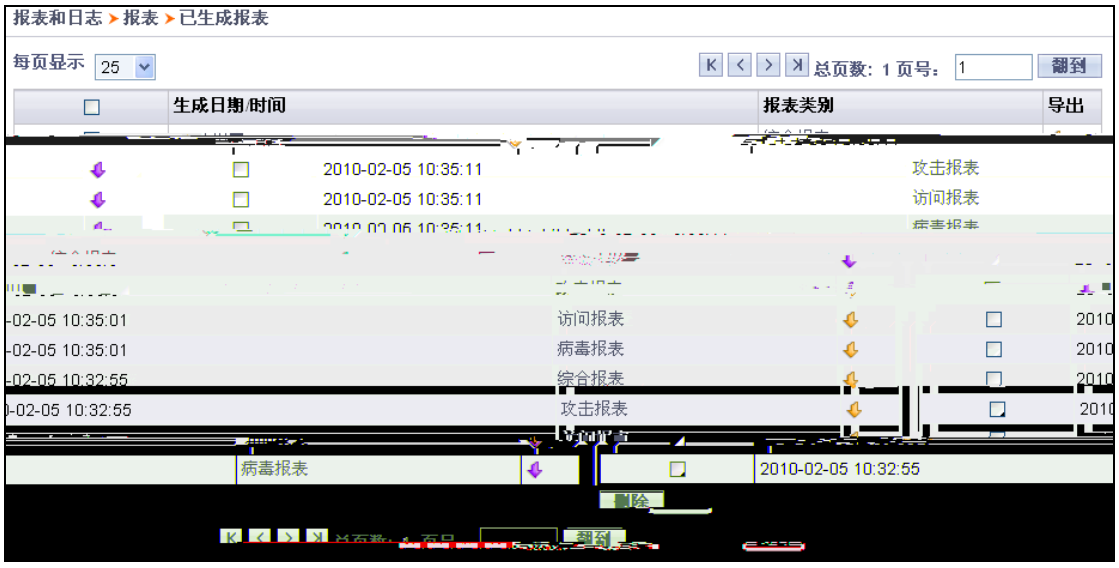
	CPU
	N
	N
	N

PC

4.1.1

“ ”

1 > >


报表和日志 ➤ 报表 ➤ 已生成报表
每页显示 25
总页数: 1 页号: 1
翻到
生成日期/时间
报表类别
导出
2010-02-05 10:35:11
攻击报表
2010-02-05 10:35:11
访问报表
-02-05 10:35:01
访问报表
-02-05 10:35:01
病毒报表
-02-05 10:32:55
综合报表
-02-05 10:32:55
攻击报表
病毒报表
2010-02-05 10:32:55
删除
翻到

2

“ ”

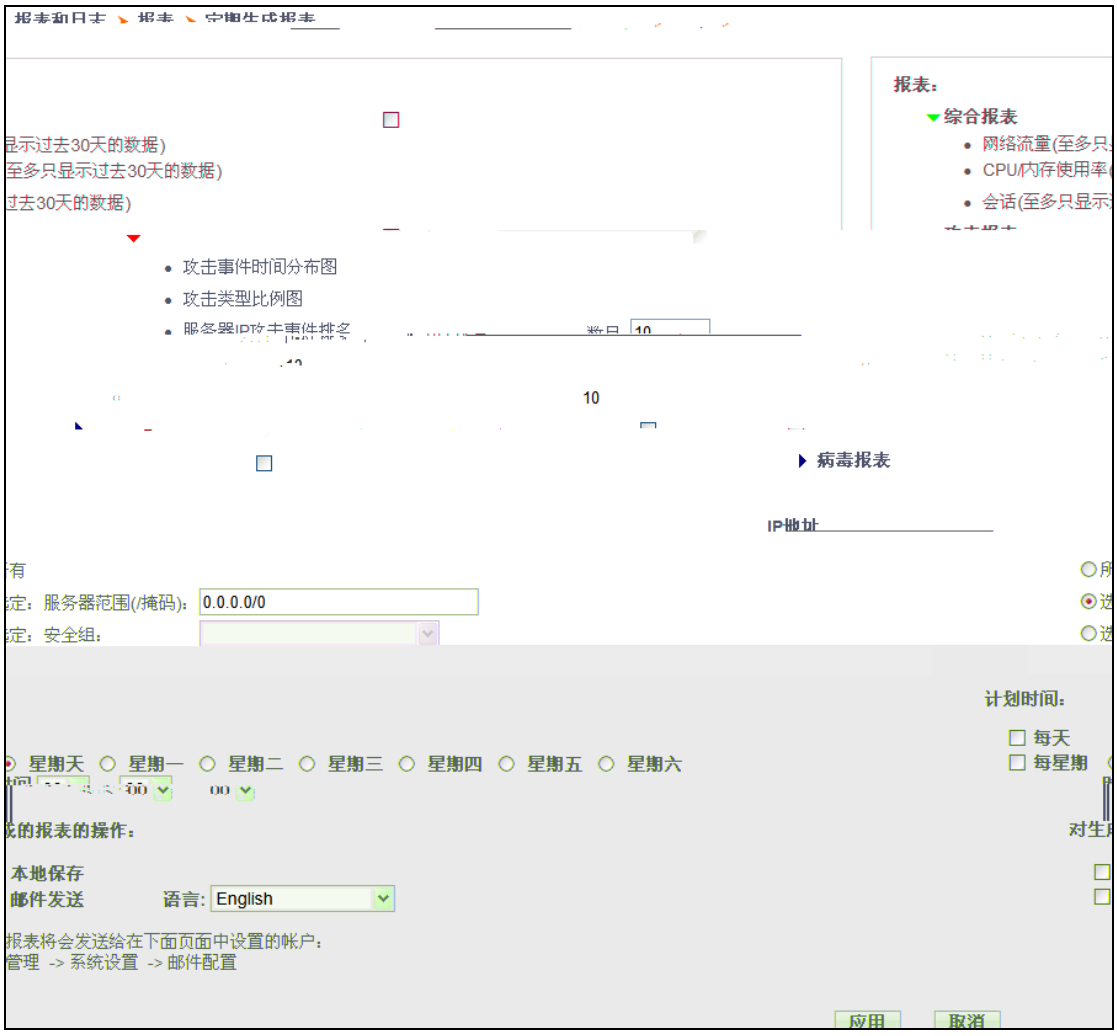
3 “ ” PC

4 “ ”

4.1.2

7.1.4

1 > >



2 “ ” “ ” “ ” “
” “ ”
“ ” “ ”

3

“ ”

“
/ ” IP

4

“ ”

A “ ” “ ” “ 7 ” “ 14 ” “ 30 ”

“ ”

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

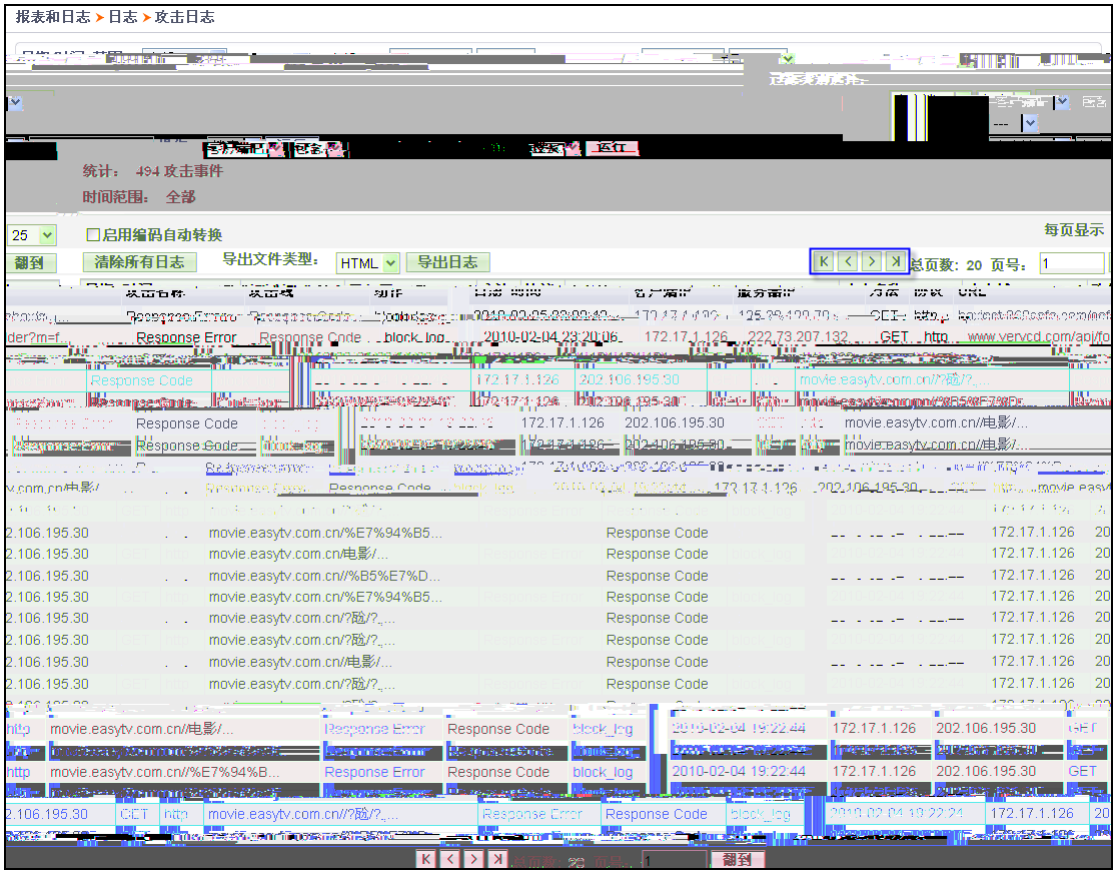
WEB

IP WEB

Cookie

http

1 > >


报表和日志 > 日志 > 攻击日志
统计： 494 攻击事件
时间范围： 全部
启用编码自动转换
每页显示
清除所有日志
导出文件类型：
HTML
导出日志
总页数: 20 页号:
Response Code
Response Error
block_log
2010-02-04 19:22:44
172.17.1.126
202.106.195.30
GET
http
movie.easytv.com.cn/电影/...
movie.easytv.com.cn/%E7%94%B5...
movie.easytv.com.cn/%B5%E7%D...
movie.easytv.com.cn/?题/?_...

“ ”

>

“ ”

25 “ ”

“ ” “ ”

2

B “ ”

“

” “ ”

“ ” “ ”

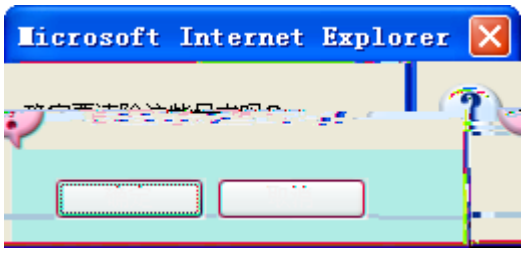
C “ ” “

” “ ”

D “ ”

“ ”

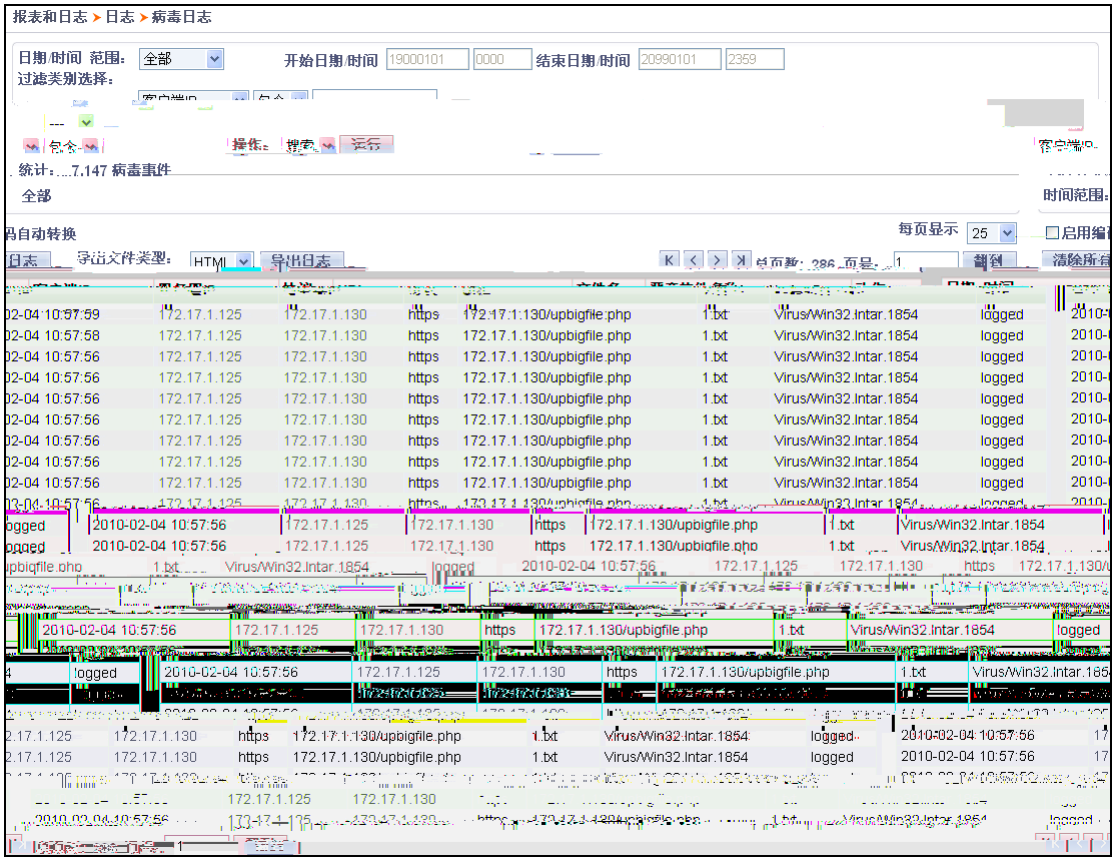
“ ”



4.2.2

“ ” WEB

1 > >


报表和日志 > 日志 > 病毒日志
日期/时间 范围: 全部
开始日期/时间 19000101 0000
结束日期/时间 20990101 2359
过滤类别选择:
操作: 搜索 运行
统计: ...7,147 病毒事件
全部
时间范围:
每页显示 25
日志 导出文件类型: HTML 导出日志
清除所有
2010-02-04 10:57:56 172.17.1.125 172.17.1.130 https 172.17.1.130/upbigfile.php 1.txt Virus/Win32.Intar.1854 logged

“ ”

>

“ ”

25 “ ”

“ ” “ ”

2

B “ ”

“

” “ ”

“ ” “ ”

C “ ” “

” “ ”

D “ ”

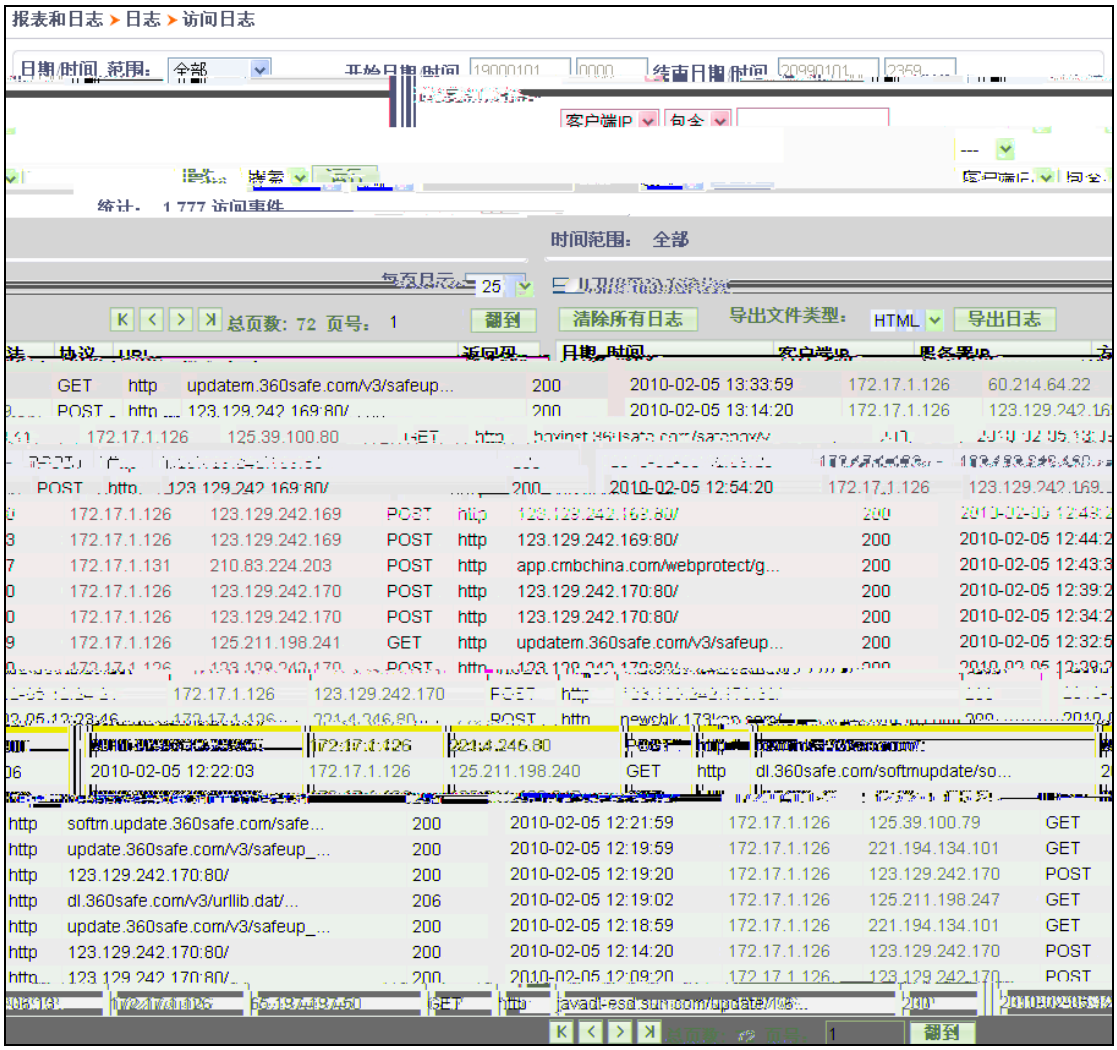
“ ”

“ ”

4.2.3

WEB

1 > >



“ ”

>

“ ”

25 “ ”

“ ” “ ”

2

	WEB
IP	WEB IP

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 ”

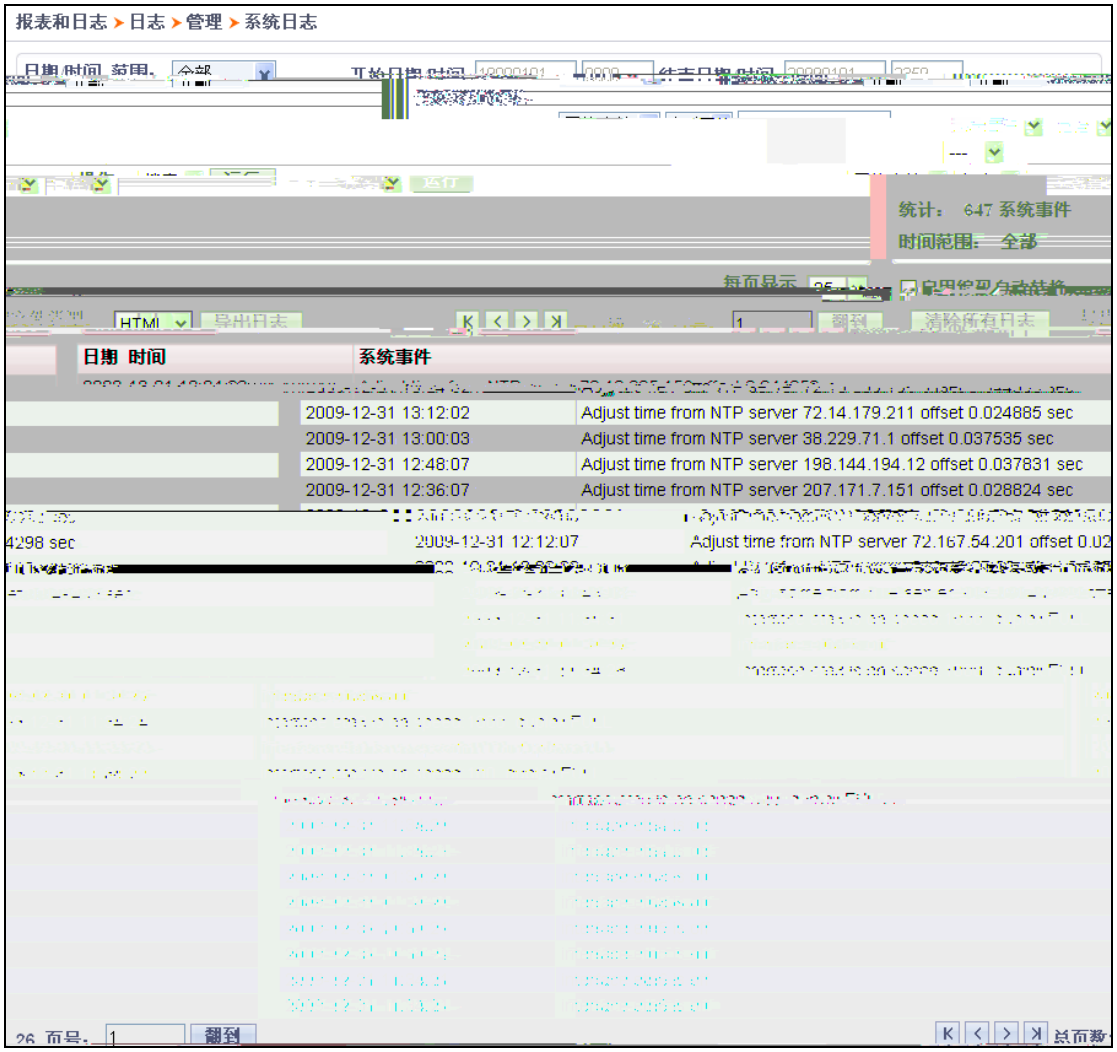
“ ” 1 00:00:00

“ 30 ” 30

“ ” “ / ” “ / ”

1

B “ ”


报表和日志 > 日志 > 管理 > 系统日志
统计： 647 系统事件
时间范围： 全部
HTML
日期 时间
系统事件
2009-12-31 13:12:02
Adjust time from NTP server 72.14.179.211 offset 0.024885 sec
2009-12-31 13:00:03
Adjust time from NTP server 38.229.71.1 offset 0.037535 sec
2009-12-31 12:48:07
Adjust time from NTP server 198.144.194.12 offset 0.037831 sec
2009-12-31 12:36:07
Adjust time from NTP server 207.171.7.151 offset 0.028824 sec
4298 sec
2009-12-31 12:12:07
Adjust time from NTP server 72.167.54.201 offset 0.02
翻到

“ ”

>

“ ”

25 “ ”

“ ” “ ”

2

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 “ ”

“ ”

“ ”

5 WEB

WEB URL

WEB

WEB URL URL POST Cookie

Webshell WEB Webshell

WEB

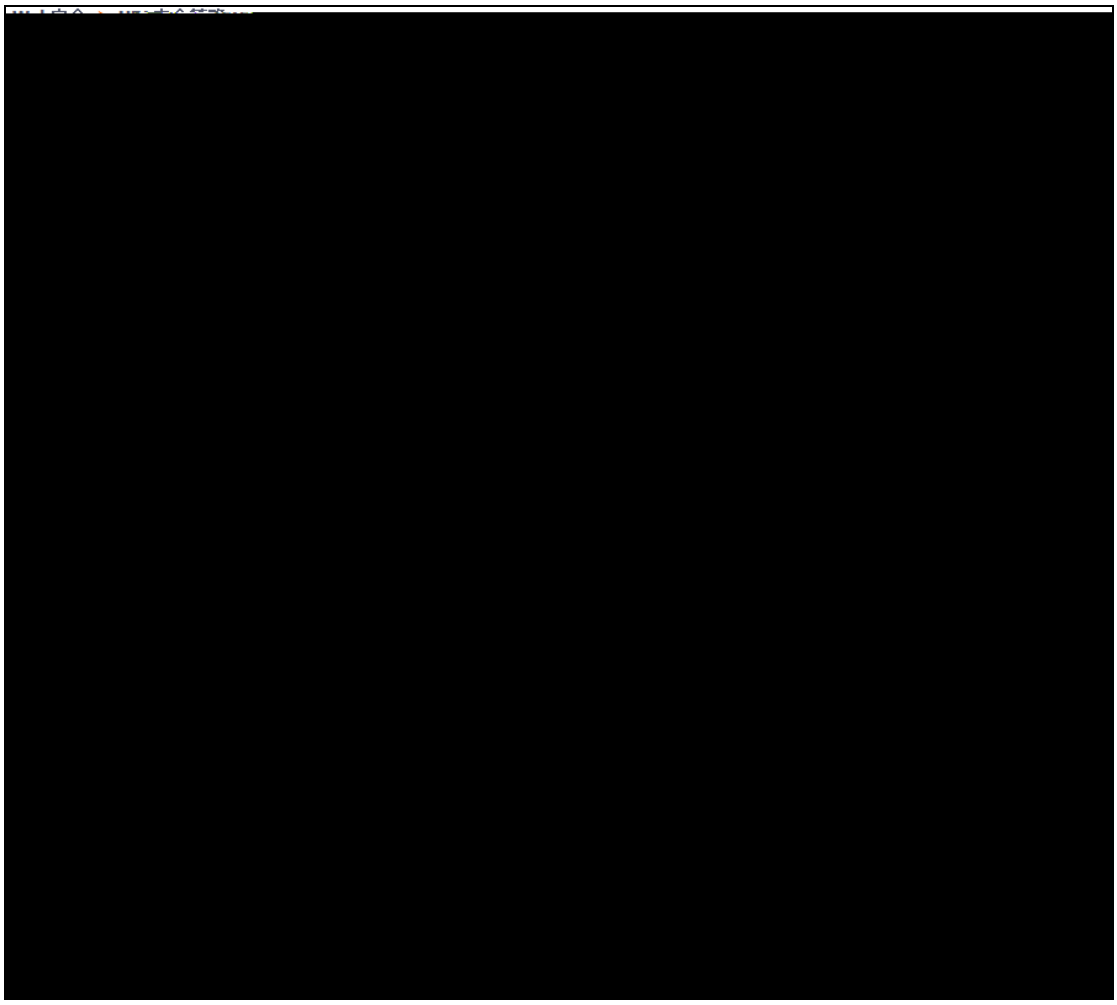
URL

1 **WEB > URL**

“ ” “ ”

2

a “ ”



b “ ”

RG-WG “ ” “

” “ ”

Web	WEB WEB 4.2.3

SQL

1

Web

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

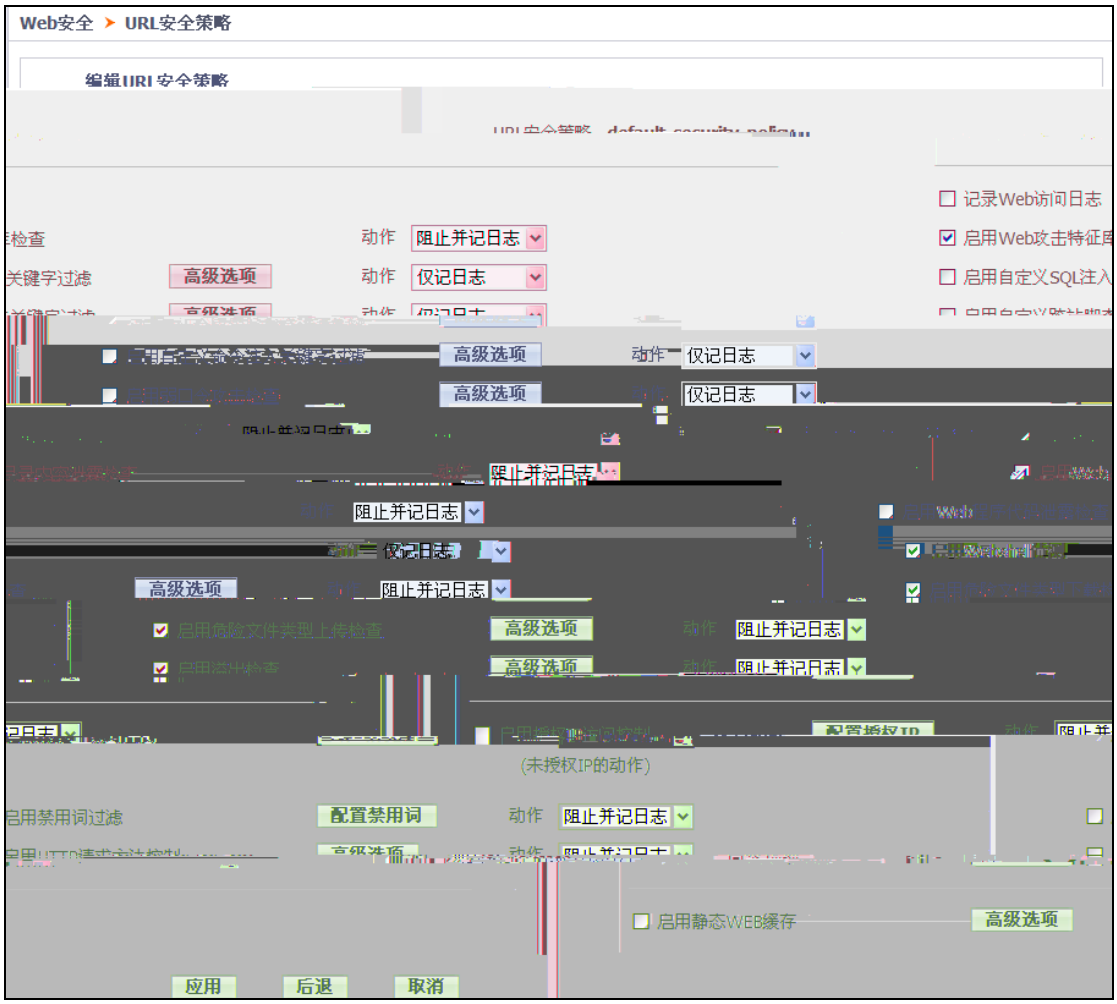
WEB

c “ ” “ ” URL

“ ”

3

“ ” “ ”



4 URL

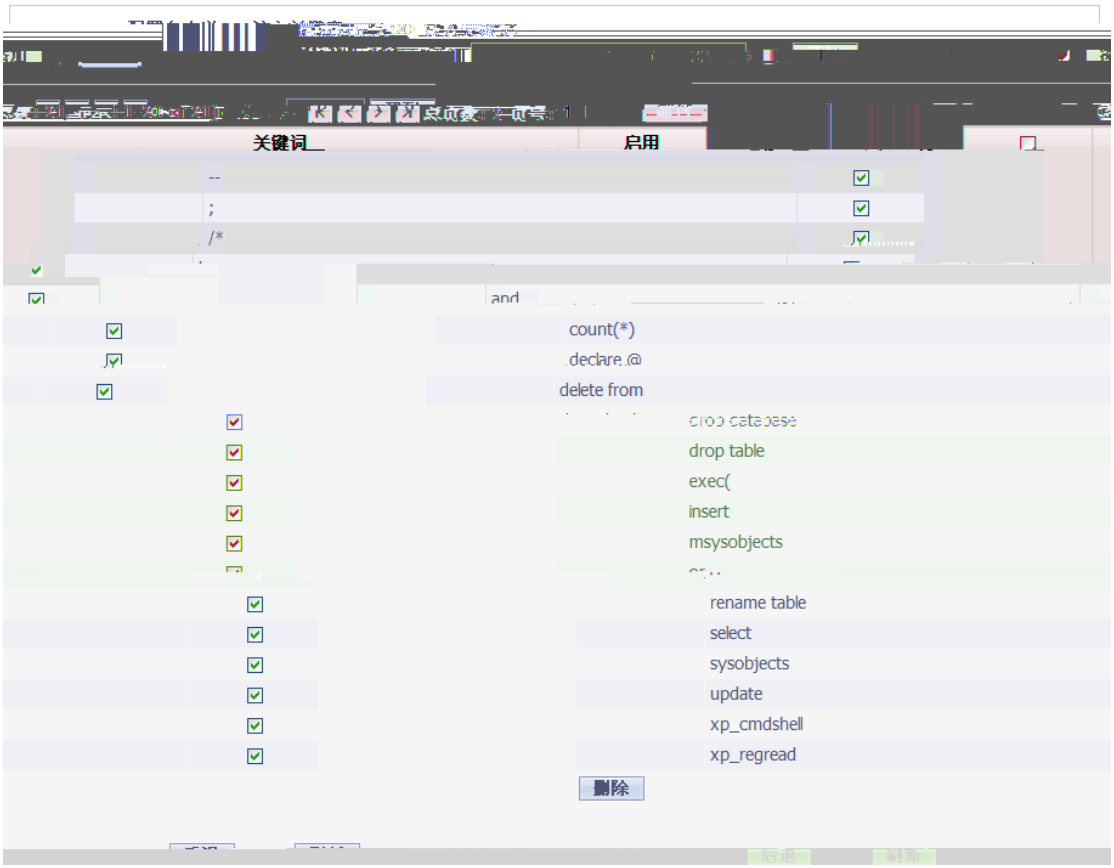
RG-WG URL

“ ”

1 “ Web ”
SQL “ ”

2 “ SQL ” WEB
SQL “ ”

3 “ ” SQL


关键词_
启用
--
;
/*
and
count(*)
declare @
delete from
drop database
drop table
exec(
insert
msysobjects
rename table
select
sysobjects
update
xp_cmdshell
xp_regread
删除

,

A Web B

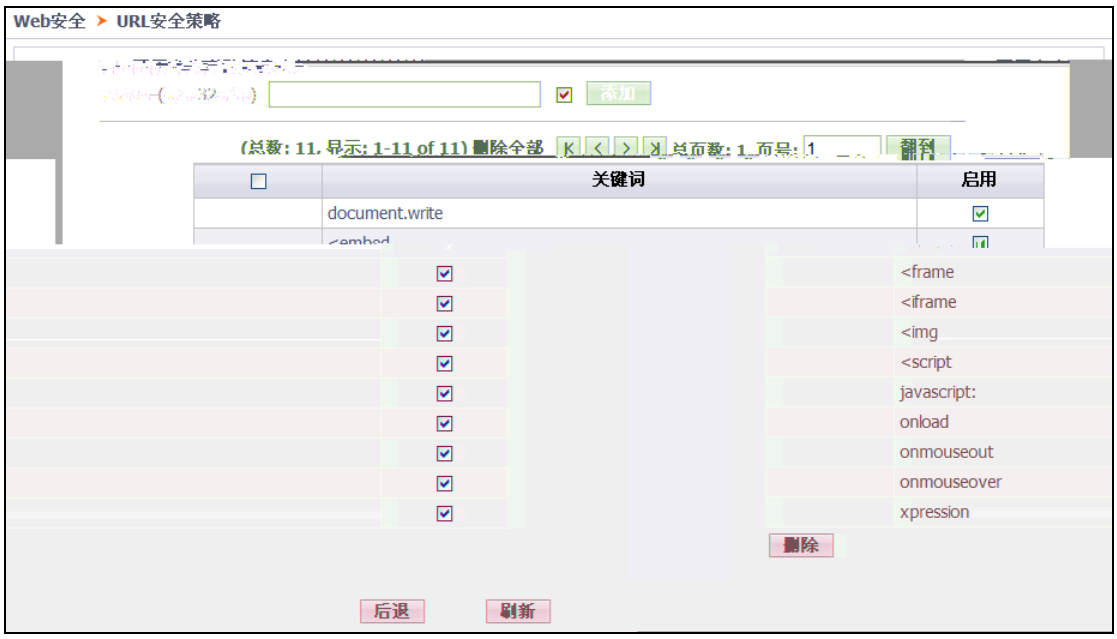
CGI

HTML

Cookie

RG-WG

3 “ ”

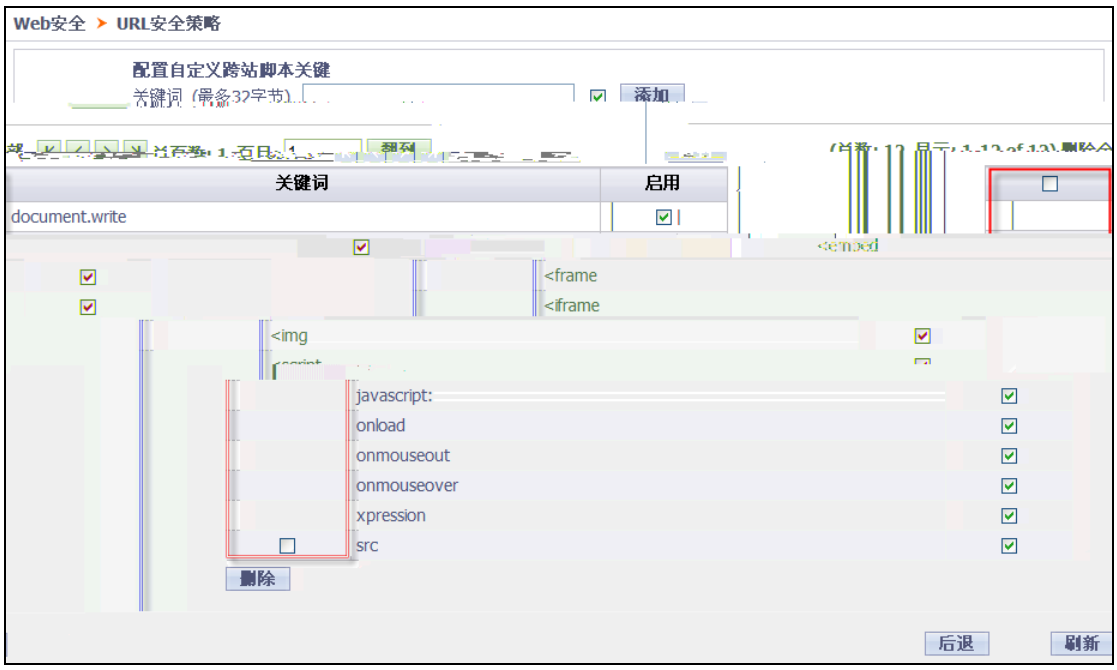

Web安全 ➤ URL安全策略
添加
(总数: 11, 显示: 1-11 of 11) 删除全部
总页数: 1 页号: 1
翻到
关键词
启用
document.write
<frame
<iframe
<img
<script
javascript:
onload
onmouseout
onmouseover
xpression
删除
后退
刷新

“ ”

A

“ ”

“ ”



B

“ ”

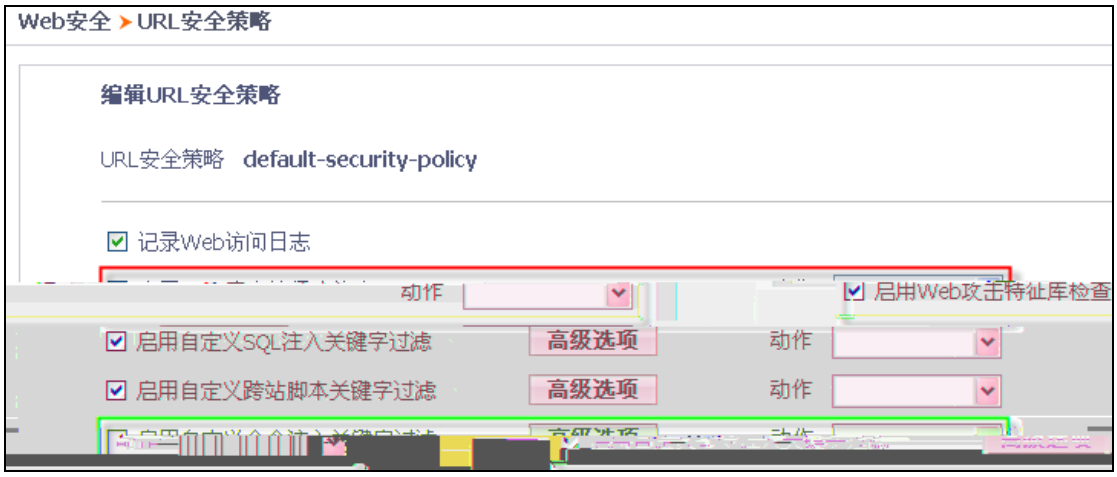
5.1.3

HTML

( )

RG-WG

URL


Web安全 ➤ URL安全策略
编辑URL安全策略
URL安全策略 default-security-policy
记录Web访问日志
动作
启用Web攻击特征库检查
启用自定义SQL注入关键字过滤
高级选项
动作
启用自定义跨站脚本关键字过滤
高级选项
动作

1 “ Web ”

“ ”

2 “ ”

3 “ ”

“ ” “ ”

“ ”

5.1.5

WEB

RG-WG WEB

“ WEB ” RG-WG WEB

“ ”

“ ” “ ” “ ”

“ ”

“ ”

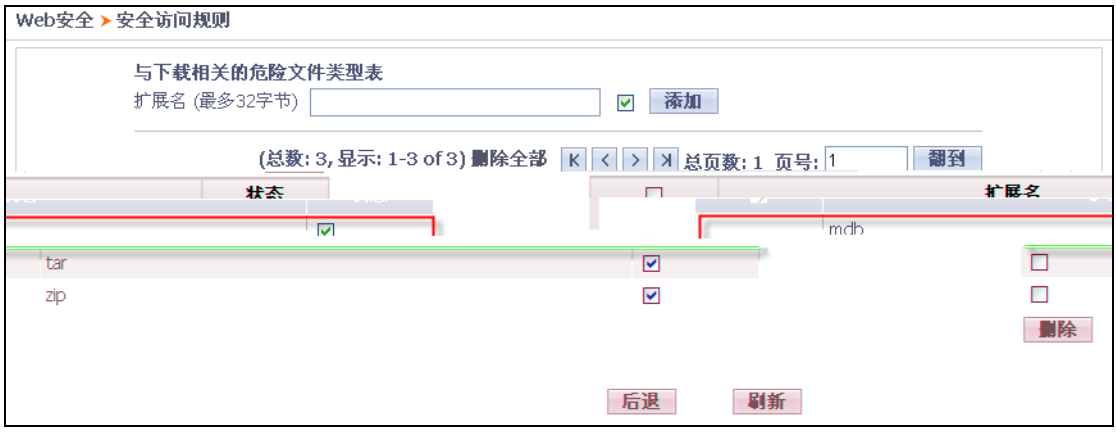
5.1.8

RG-WG

WEB

1 “ ” RG-WG “

”



“ mdb ”

WEB RG

= Ñ ˜ :e—C& .´!S $ È X Á 0P

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

“ ” WEB RG-WG

“ ” “ ”

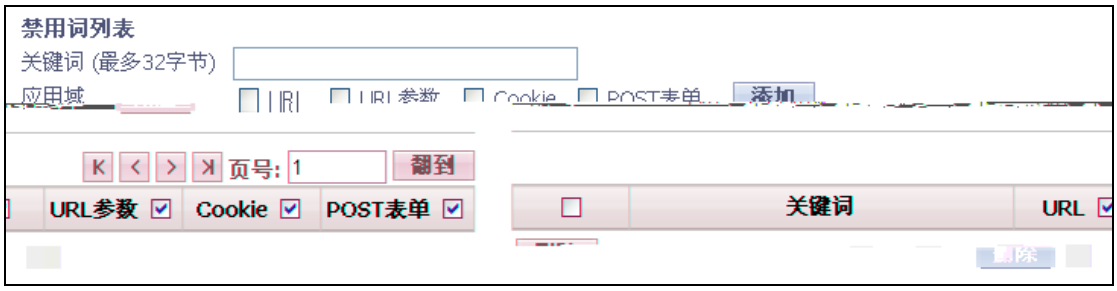
“ ” “ ” “ ”

“ ”

“ ”

2

“ ”



A

“ ” “ ”

“ URL ” “ URL ” “ POST ” “ Cookie ”

“ ”

B

“ ”

C

RG-WG HTTP

2

“ ”

A “ ” “ ”
“ ” WEB FTP IP
WEB

B “ ” WEB

C “ URL ” ŗ ŗ

34Dm70Imag1C4> 3 TJ EEMC /P <</MCID 19>> BDC BT /F30310.56 Tf 1 0 0 1 192.17 657.58 T479[(C)m70Imag1C4>]MC

“ ”

3

“ ” “ ”

“ ” “ ” “ ” “

”

4

05.42 7pe/Pa /P> BDMCID 203842 78q Tm[<315f96 0ETBT1 013ET2 5ET39BT220r T24Tw56[<5E4D>-756 Tf2E183-7523F762986B08>1 505.


Web安全 ➤ 服务器安全组
配置URL黑名单
(最多255字节)
添加
URL
编号
后退
刷新

“ URL ” WEB URL
path level URL “ ”

URL

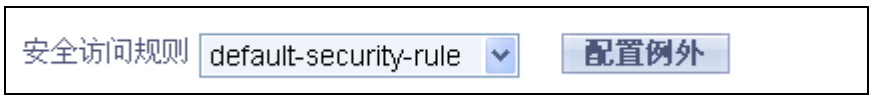
www.sina.com URL

“ ”

5.2.4 URL

URL Web
URL URL
URL URL URL URL
5.1URL

1 WEB URL

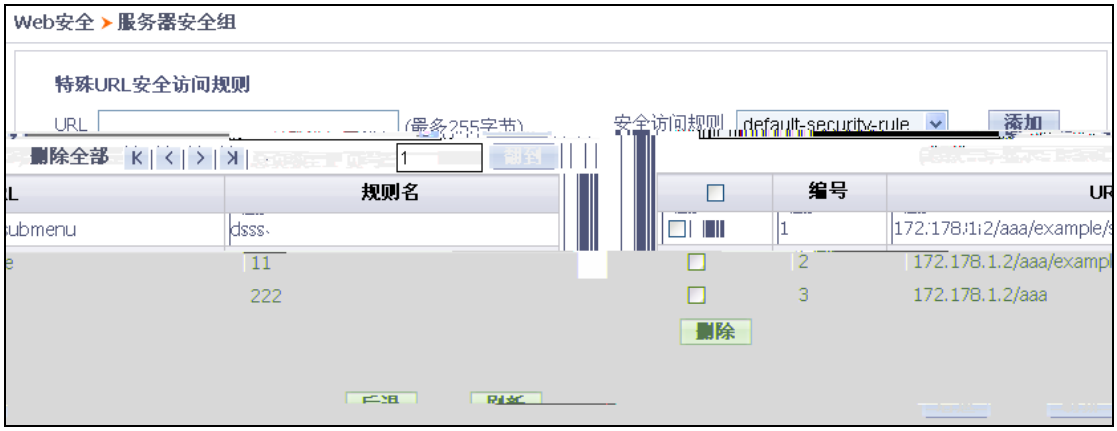


2

URL “
” URL

A

“ URL ” URL “ URL ”
“ URL ” “ ”



B

“ ”

5.2.5

RG-WG WEB
FTP

1 “ ” “ HTTP
” “ FTP ” “ RG-WG
“ ”

SQL

Cookie

Cookie RG-WG Cookie

Cookie

1 **W**

RG-WG URL

<script src= ”http://domain/…… ”>, <iframe src= ”http://domain/…….. ”>

domain domain RG-WG

WEB

“ ” HTTP

1 WEB

2 WEB

3 WEB

UDP Flood

ICMP Flood

Dos RG-WG Dos

1 **Web**

5.5 WEB

RG-WG

“ ” WEB

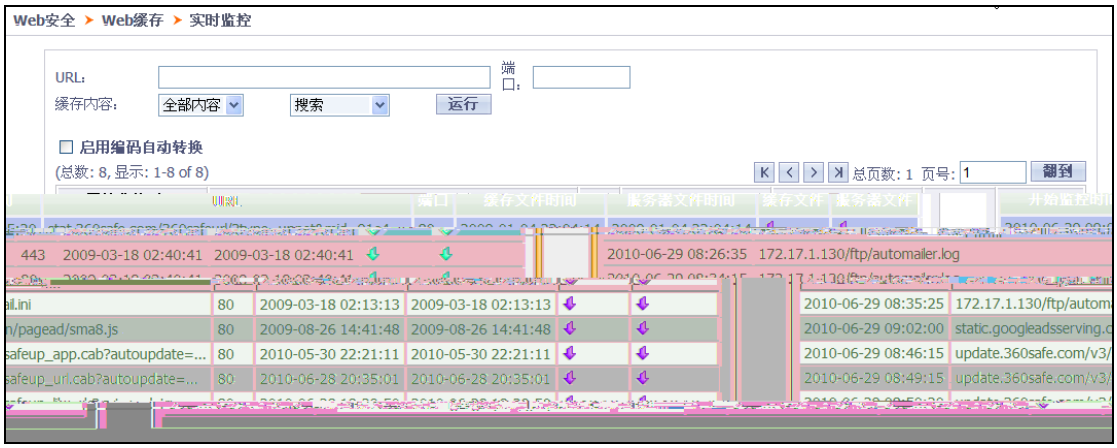
GB 1-50

2 “ ”

5.5.2

5.5.1

1 **Web** > **Web** >



“ ”

>

“ ” “ ”

“ ” “

”

2

“ URL ” “ ”

5.6

WEB HTTPS HTTPS

certificate

Web

WEB

RG_WG 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: 10 (1-7200) 分钟
在攻击日志中记录事件
应用
动态攻击黑名单
解锁
下面的IP将不会被加入动态攻击黑名单
客户 IP/子网掩码:
添加
页号: 1
翻到
源IP/子网掩码
删除
刷新

2

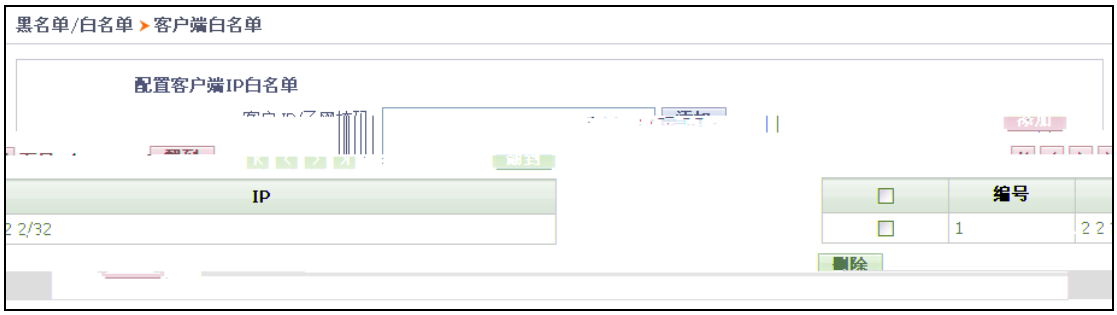
“ ɦ ɹ ɲ ”

6.3

IP

2
WEB

1 / >



2

“ IP ”

È

7

7.1

7.1.1

1 > > [illegible]

2 “ ”

3 “ ”
“ ǰ

7.1.2

Ų ǰ ۪

7.1.2.1

“ ”

“ ”

‘ ’

“ ”

7.1.2.2 SNMP

SNMP

3 SNMP
SNMP SNMP

a > >

b SNMP

c “ ” “ SNMP ”

d “ ”

7.1.2.3

1

“ ”

2

7.1.3.1

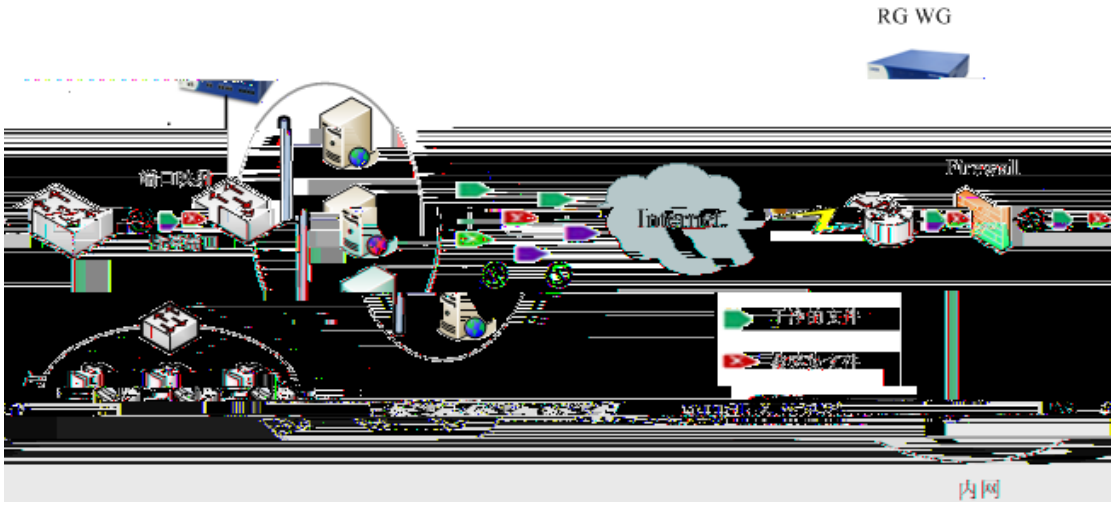
WEB WEB

HTTP/HTTPS

WEB WEB

WEB

SPAN



span

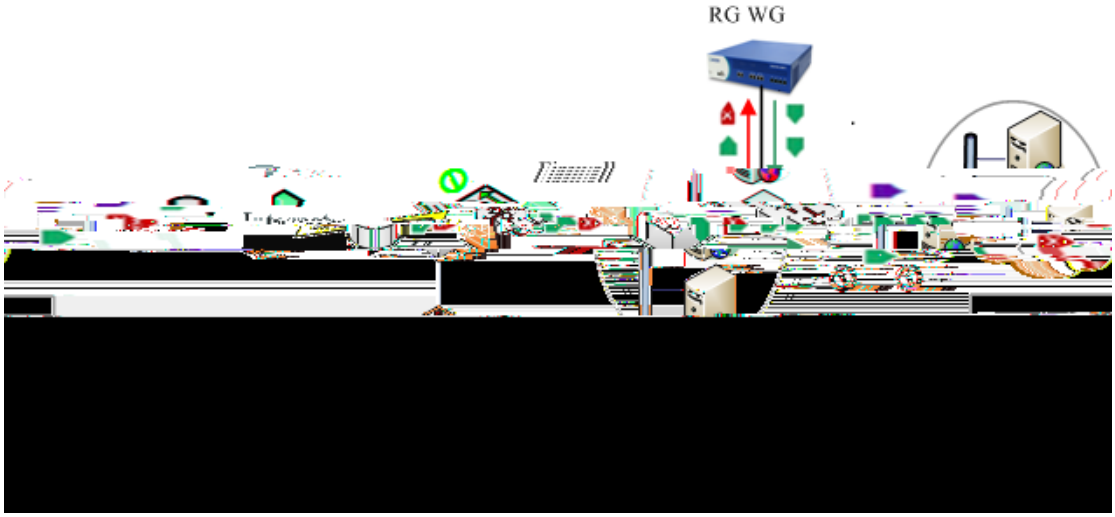
- WEB
-

RG_WG

WEB Web

Web RG_WG

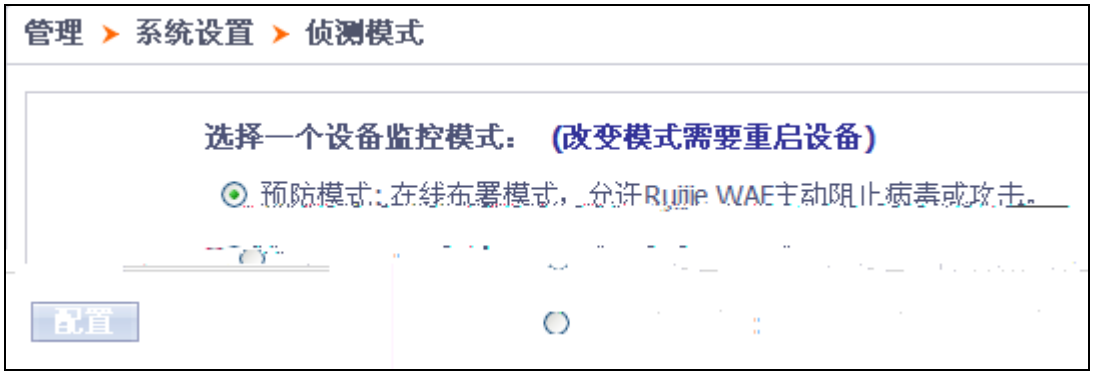
Web


RG WG

WEB

1 > >

2


管理 ➤ 系统设置 ➤ 侦测模式
选择一个设备监控模式： (改变模式需要重启设备)
预防模式：在线布署模式，允许Ruijie WAE主动阻止病毒或攻击。
配置

“ ”

A > >

B > >

IP

C “ ”

IP WEB IP

“ ”

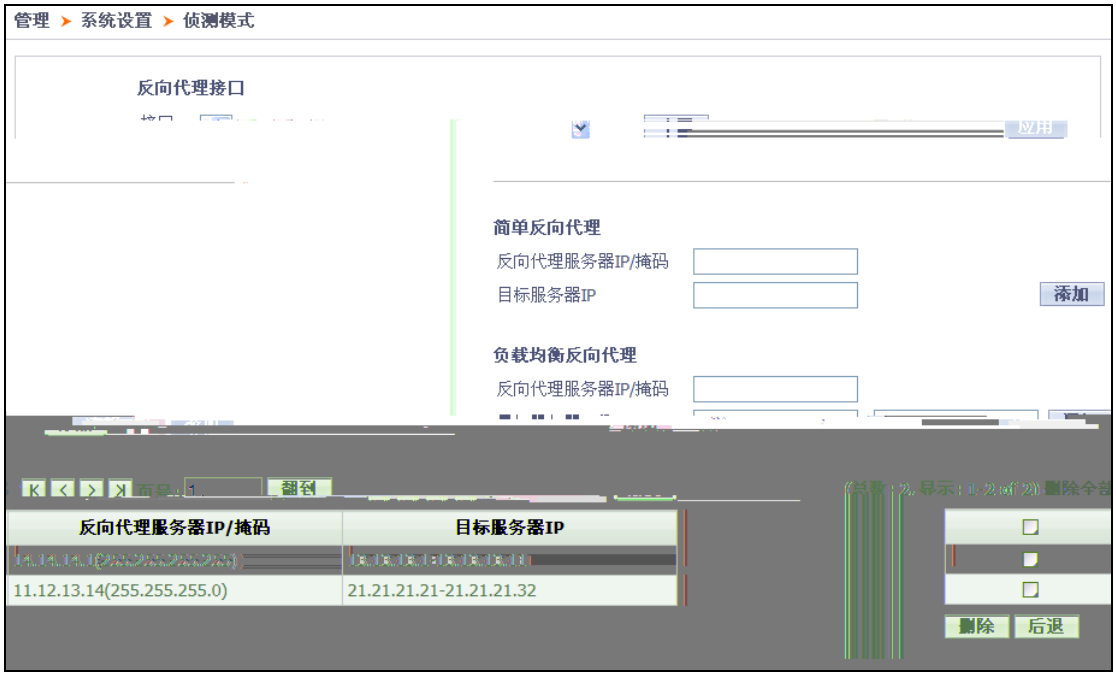
Web “ ” RG_WG

“ IP/ ” RG_WG WEB

IP

“ IP ” RG_WG Web IP

“ IP ” WEB IP



3 “ ”

4

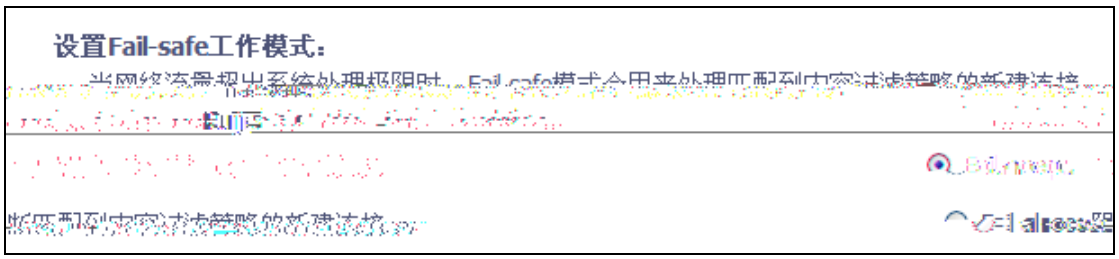
7.1.3.2

RG-WG bypass

failopen

WEB

1 > >



2

Fail-open WEB

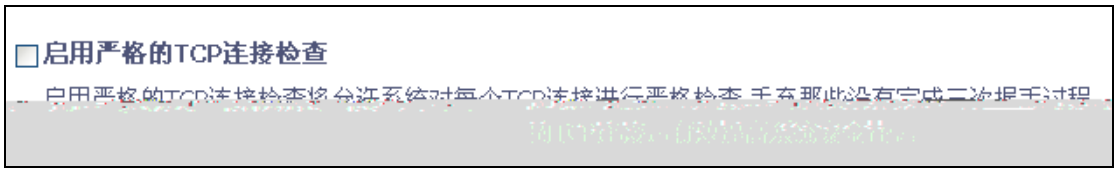
Fail-close

7.1.3.4 TCP

TCP TCP
TCP

1 > >

2 “ TCP ”



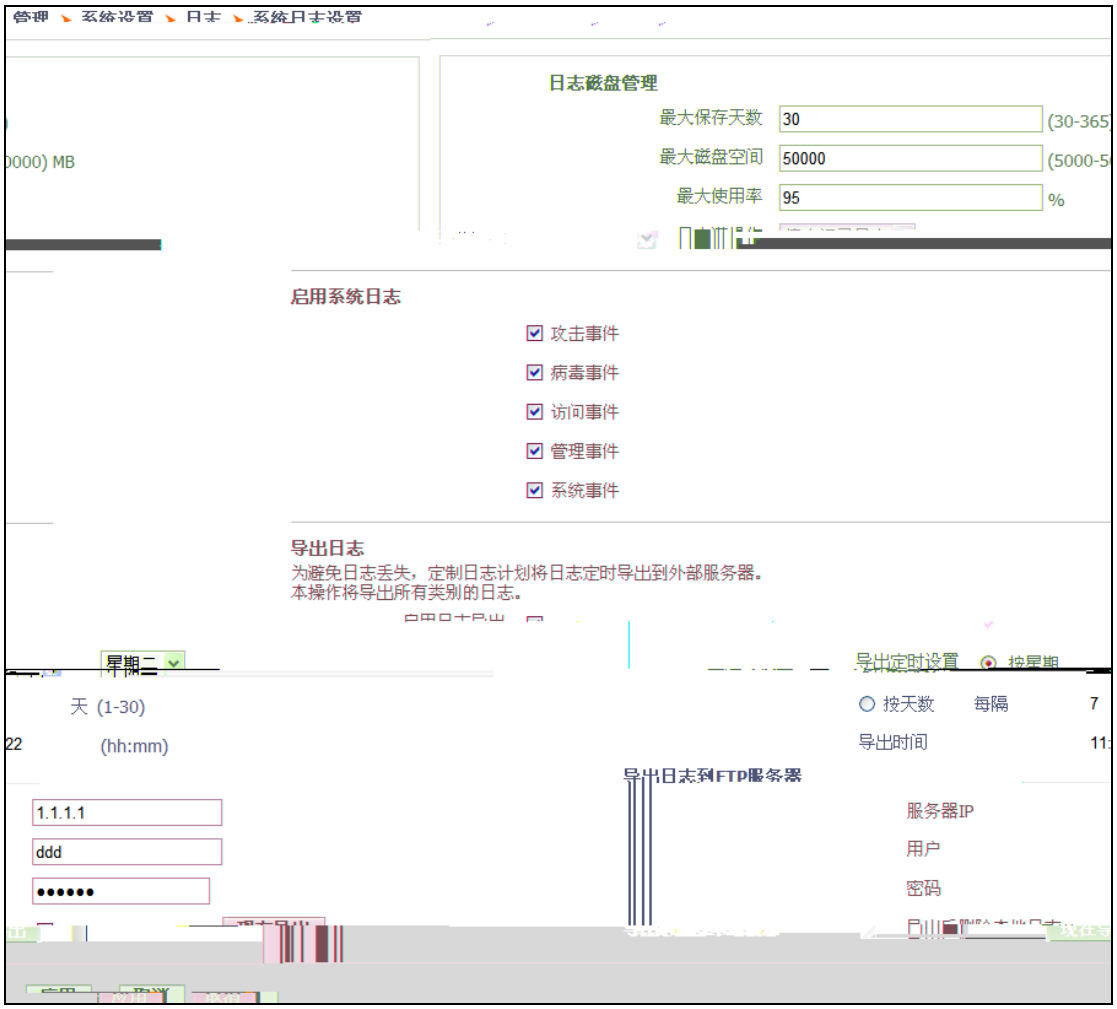
3 “ ”

7.1.4

WEB
HA
QMAIL

2

1 > >



2

	5000-50000 MB

1

	4 4.2.4 5 HA 4.2.5

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

“ ”

SNMP SNMP Trap

SNMP Trap

3 “ ”

7.2

7.2.1

4 8 8

RG-WG 2

IP TCP

IP

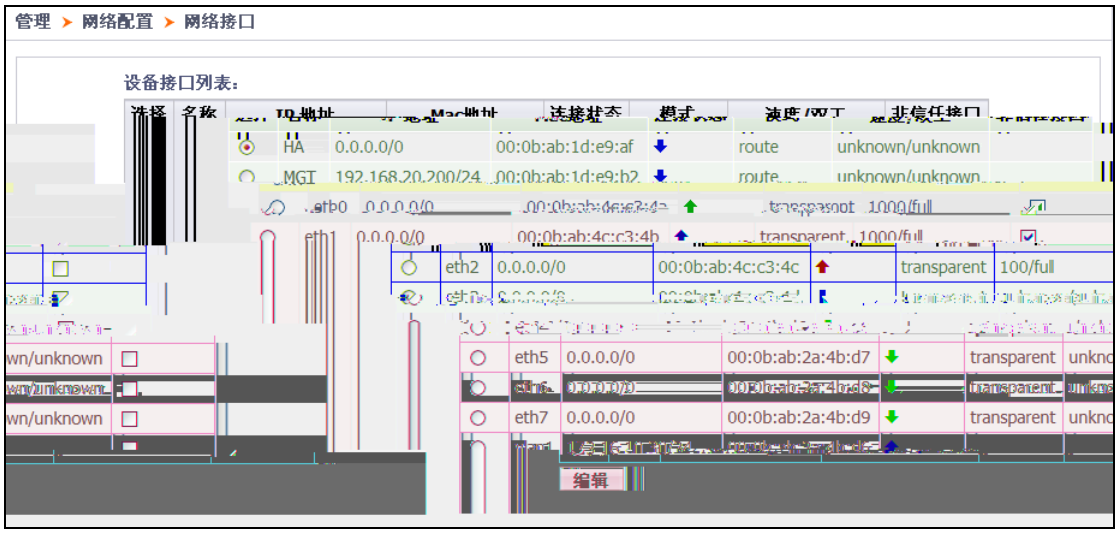
RG-WG WEB ASIC

WEB

WEB

7.2.1.2

1 > >



VLAN HA

HA RG-WG2000

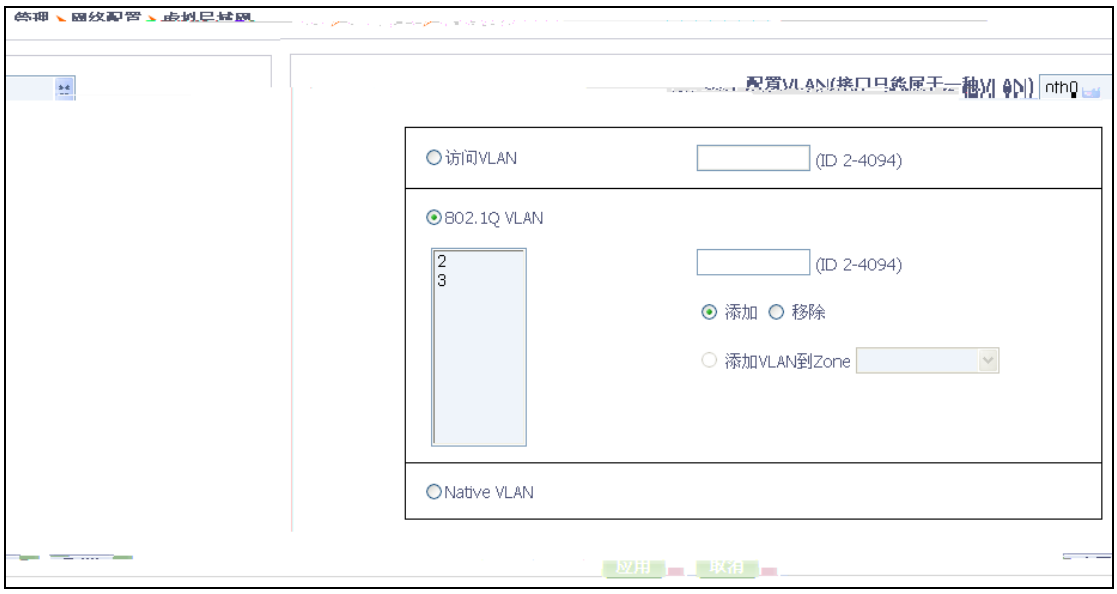
RG-WG3000 ő RG-WG1000

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

VLAN 1 VLAN 1

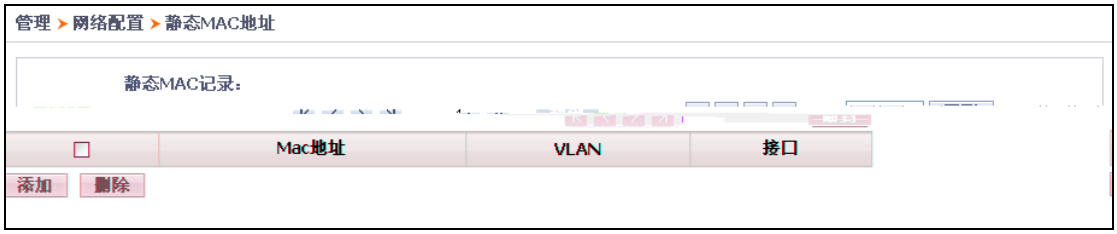
“ Native VLAN ” “ ”

7.2.3 MAC

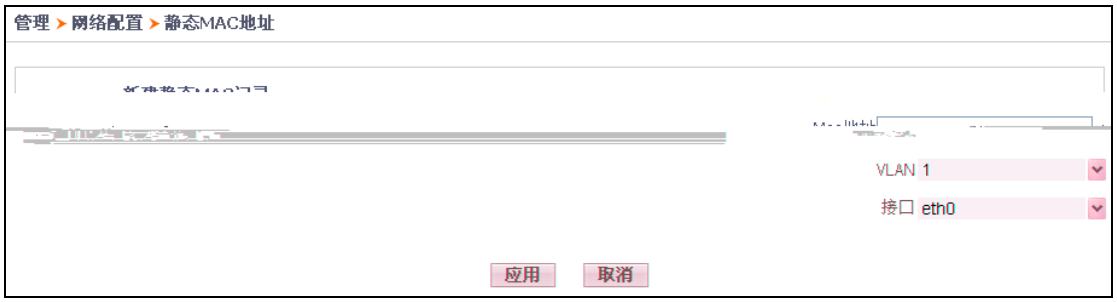
MAC

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

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

1-32

VRRP

2 “ ”

:

IP

7.3.1.2

WEB

1 > > >

WEB

a > > >

b “ ” “ ” “ WEB
” “ ”

5

a > > >

b “ ” “ ” “ WEB
” “ ”
“ ”

6

“ ” “ WEB
” “ ” “ ”
“ ”

Web “ ”

”

1 > > >

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

2 “ ”

7.3.2

WEB

RG-WG 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 administrator WEB
CLI

7.4.1

WEBUI CLI
RG-WG

——

“ ”

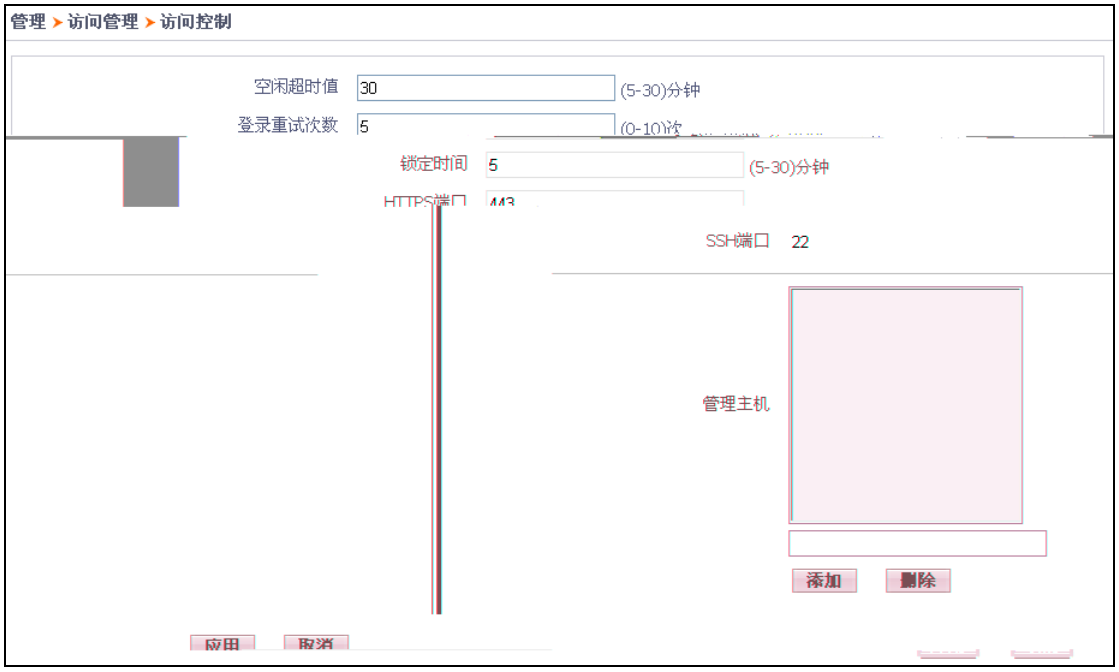
	“ ”
	Read-write —— Read-only —— Audit ——

3 “ ”

7.4.2

HTTPS SSH

1 > >



	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