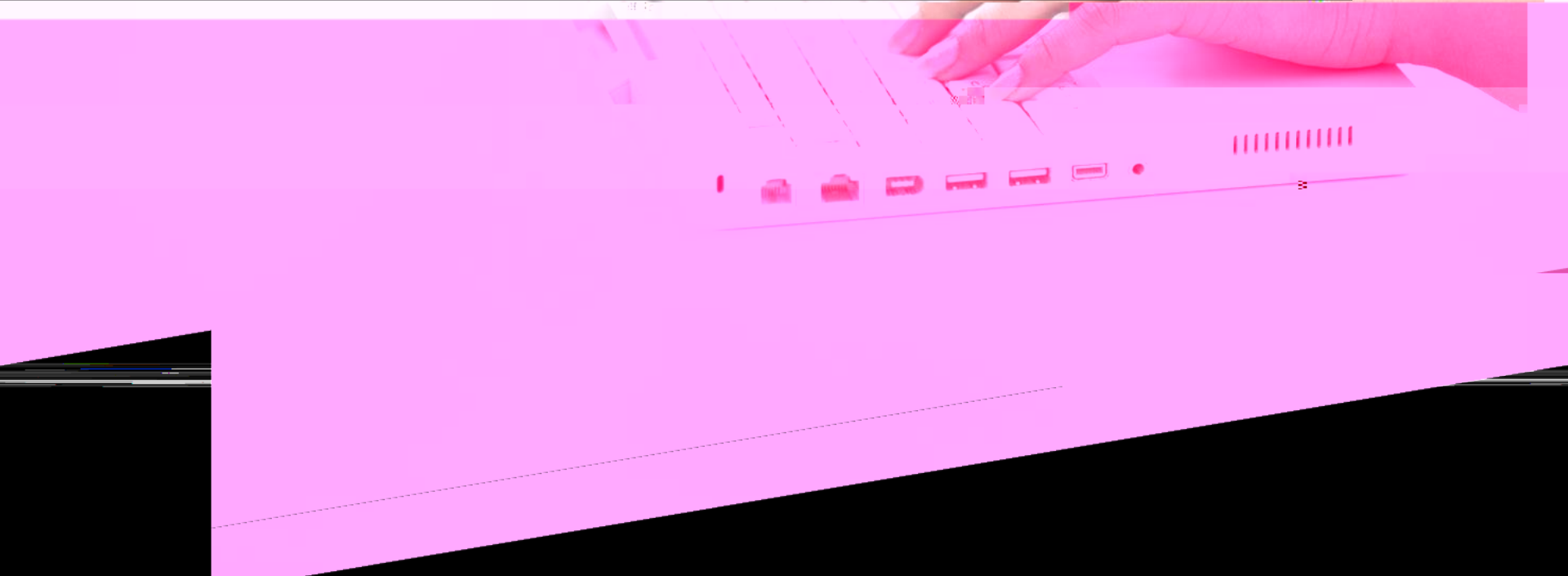
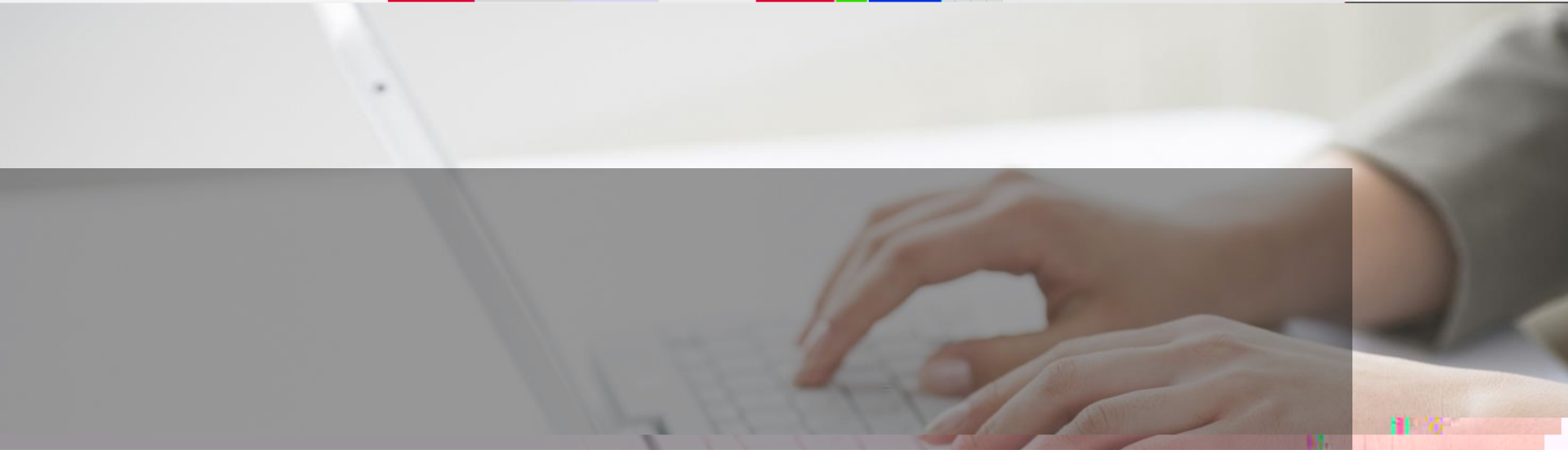
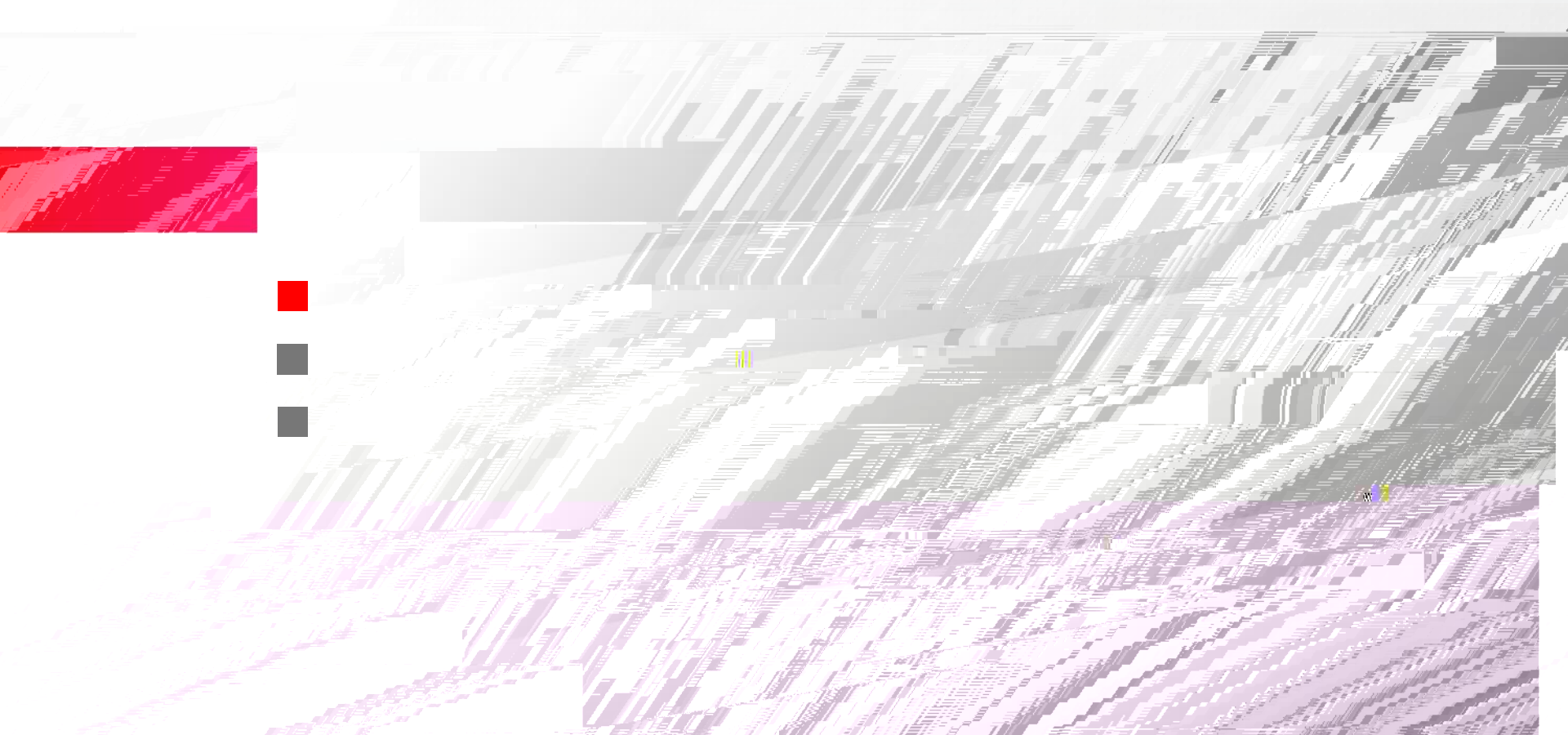






1
2
3

web

1
2
3
4

WG

WG

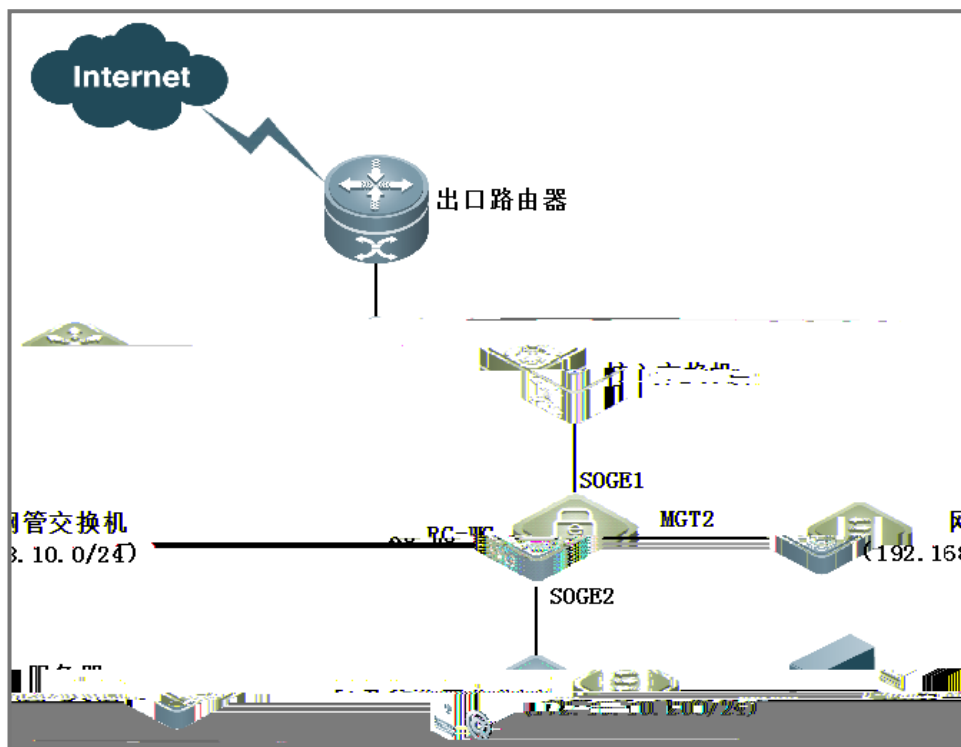
IP

MAC

PPT

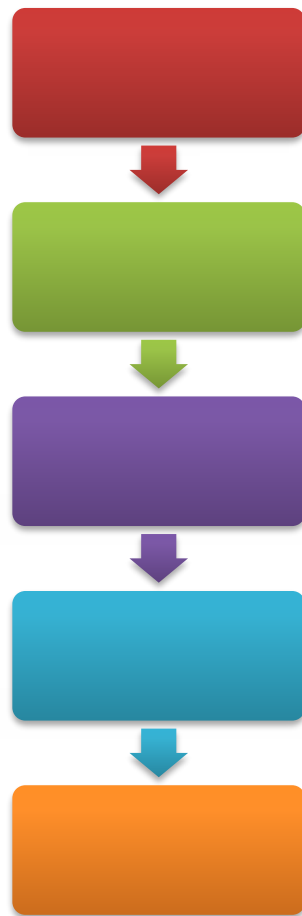
RG-WG

WebGuard



WG

5





->

->

bridge2

2-4094

+ Port接口 + Channel接口 + 网桥接口 + Trunk接口							增加+	刷新	设置
名称	IP地址	子网掩码	MTU	模式	状态				
MngtBridge	192.168.1.200	255.255.255.0	1500	普通模式	启用				

->

->Port

port

S0GE1

S0GE2

bridge2

+ Port接口 + Channel接口 + 网桥接口 + Trunk接口					
☐ 接口名称	☐ Channel接口	☐ 网桥接口	☐ 启用状态	☐ 链路状态	
☐ MGT1	空	MngtBridge	启用	启用	
☐ S0GE1	空	bridge2	启用	启用	
☐ S0GE2	bridge2	启用	启用		



“ web1> ”

+ HTTP服务器+ HTTPS服务器+ 其他服务器

增加+刷新

每页显示 15

串联	代理模式	bridge2	开启
☐	web1	172.16.10.200	80

<1>

当前 1 - 1, 总共 1 条记录

bridge2

HTTP

HTTPS

“ Web -> Web ” Web
 Web
 web -> web
 p1
 web1
 “ Web ”
 “ ” “IP ”,

Default Low

The screenshot shows the '编辑Web防护策略' (Edit Web Protection Strategy) window. It has three tabs: '基本配置' (Basic Configuration), '错误页面配置' (Error Page Configuration), and '重定向配置' (Redirect Configuration). The '基本配置' tab is active, showing the following fields:

- 名称 * (Name): p1
- 服务器 (Server): web1
- 源IP (Source IP): 空 (Empty)
- Web防护模板 (Web Protection Template): Default Low
- 访问日志 (Access Log): 关闭 (Closed)
- 优先级 * (Priority): 0
- 启用 (Enabled): ☒

At the bottom of the window, there is a status bar with a red line and a green line.

Default Low

WG



Default Low

WebUI

>>

/IP

+ 攻击日志

条件

细节

清空

导出

刷新

每页显示

15

日期和时间	源IP	源端口	站点域名/IP	目的URL	参数	方法	攻击类型	处理动作	规则号	
	GET	特征防护规则	阻断	50210	☐	2017-03-23 14:07:49	180.76.15.139	17343	mail.szit.edu.cn	/robots.txt
2017-03-23 14:07:49	GET	特征防护规则	阻断	50210	☐	2017-03-23 14:07:49	180.76.15.146	27702	authserver.szit.edu.cn	/authserver/login.aspx
1	/js/app/loginApp.js	GET	特征防护规则	阻断	40092	☐	2017-03-23 14:07:46	10.231.1.13	51222	authserver.szit.edu.cn



URL /

URL /

URL

URL

>>

URL

HTTP

URL

细节

日志详细信息

HTTP详细信息

HTTP请求

GET
/authserver/login
service=http%3A%2F%2Fsqjy.szit.edu.cn%2Fthemes%2Fhne%2F1%2F837.html
Host:authserver.szit.edu.cn
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html)
Accept: */*

HTTP请求体

匹配位置

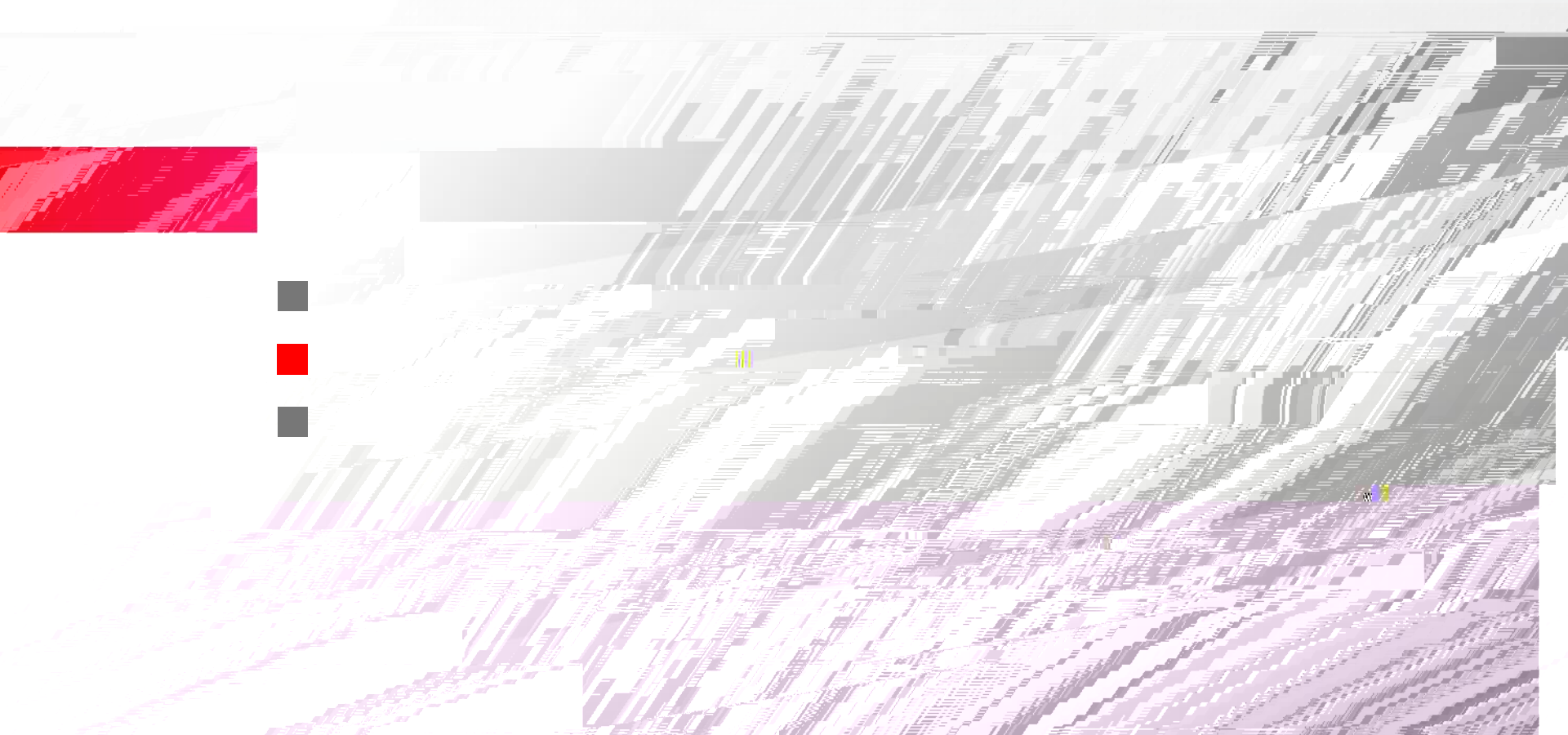
匹配特征

HTTP请求UserAgent

Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html)

Web

URL



WEB

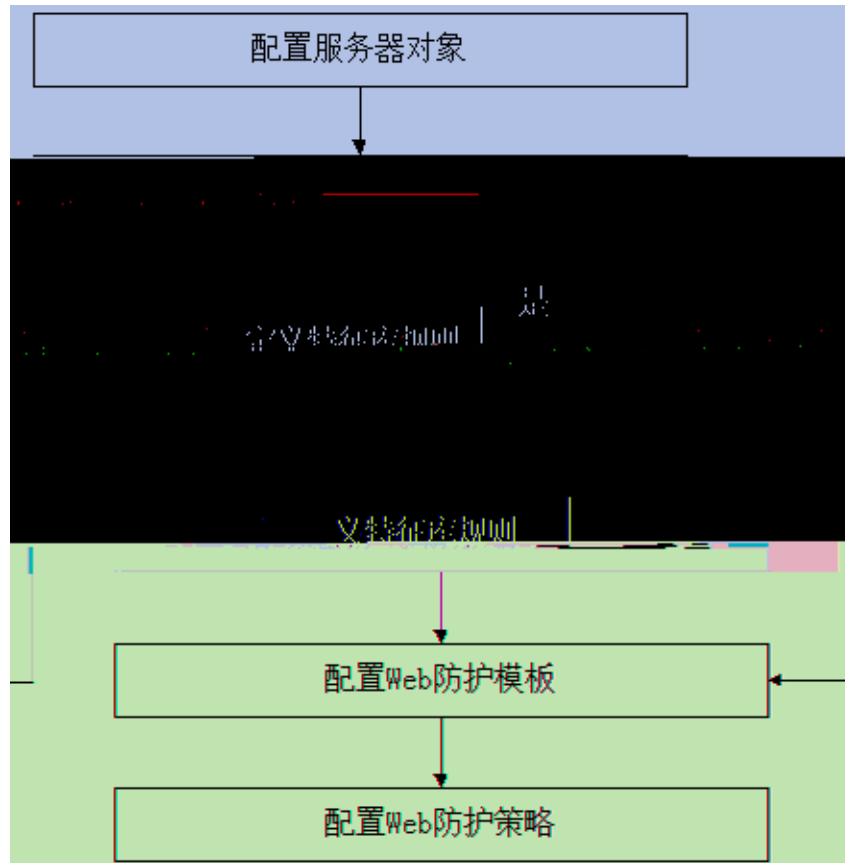
Web

IP

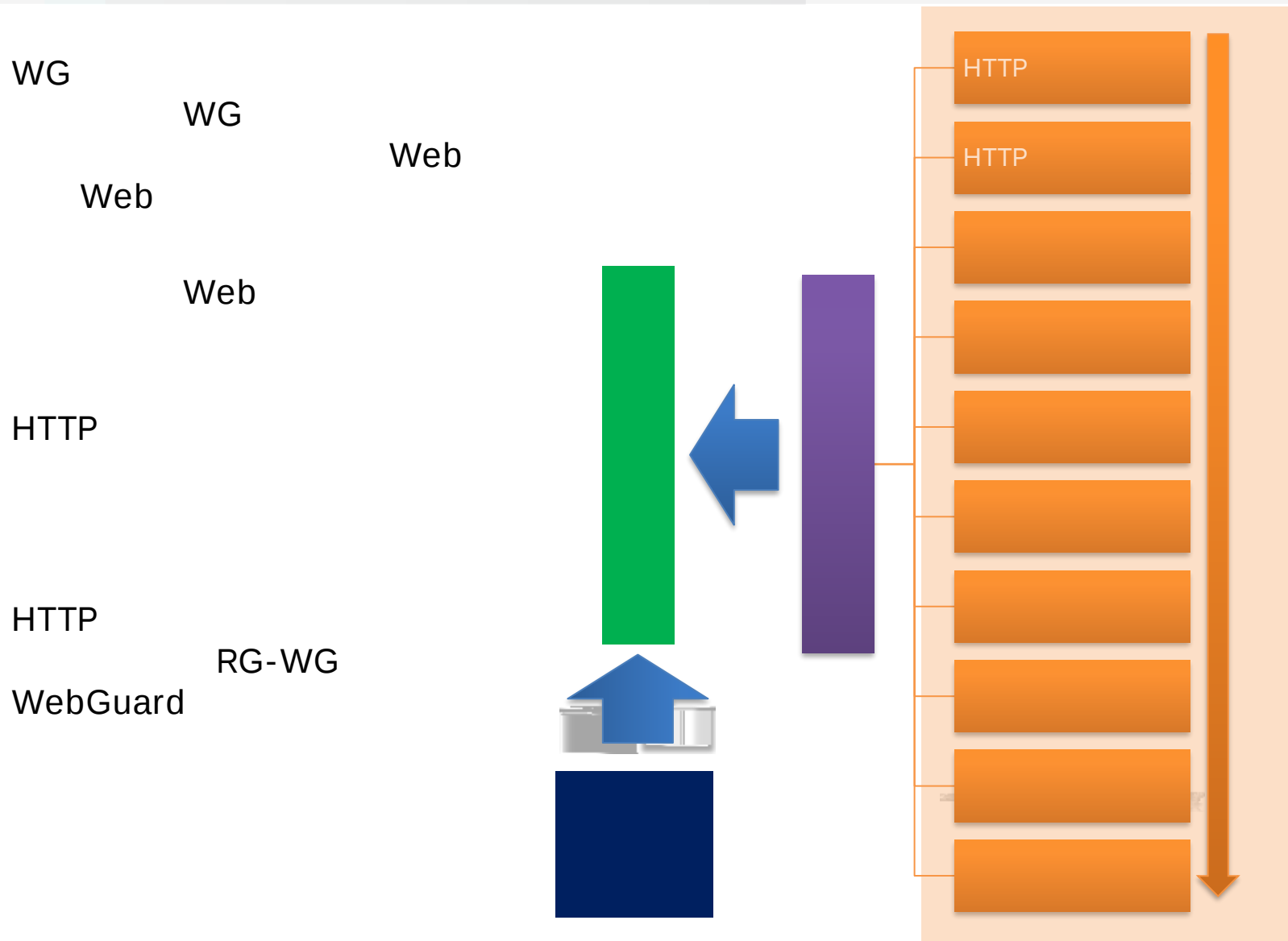
Web

Web

Web



WEB



WEB



monitor

编辑特征规则

名称 *

例外url	处理动作	告警设置	日志
☒ 跨站脚本攻击(XSS)	空 阻断	☐ 邮件 ☐ 短信	☒
☐ 防爬虫	空 阻断	☐ 邮件 ☐ 短信	☒
☐ 协议完整性	空 阻断	☐ 邮件 ☐ 短信	☒
☒ 溢出	空 阻断	☐ 邮件 ☐ 短信	☒
☐ 未定义规则	空 阻断	☐ 邮件 ☐ 短信	☒

WEB

“

web1

”

+ HTTP服务器

+ HTTPS服务器

+ 其他服务器

增加+

刷新

每页显示

15

																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																					</
-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	----------------

172.16.10.200

WEB

80

bridge2

HTTP

HTTPS

WEB

“ Web -> Web ” Web
 Web
 web -
 >web
 p1
 web1
 “ Web ”
 “ ” “IP ”,
 Default Low

Default Low HTTP WG
 WEB WG
 “ -> WEB -> WEB ”

WEB

3 404 WG WEB " -> "
1 1 WG URL <http://172.16.10.200/forum.php>

端口	站点域名/IP	目的URL	参数	方法	攻击类型	处理动作	规则号	次数	日期和时间	源IP	源
10	1	2016-12-21 01:39:38	172.16.10.188	51168	172.16.10.200	/forum.php	id=1%20and%...	GET	特征防护规则	阻断	100
10	1	2016-12-21 01:39:37	172.16.10.188	51168	172.16.10.200	/forum.php	id=1%20and%...	GET	特征防护规则	阻断	100
10	1	2016-12-21 01:39:36	172.16.10.188	51168	172.16.10.200	/forum.php	id=1%20and%...	GET	特征防护规则	阻断	100
/forum.php id=1%20and%... GET 特征防护规则 阻断 10010 1 2016-12-21 00:52:37 172.16.10.123 56781 172.16.10.100											
m.php id=1%20and%... GET 特征防护规则 阻断 10010 10 2016-12-21 00:47:51 172.16.10.123 56647 172.16.10.200 /foru											
2016-12-21 00:46:45 172.16.10.123 56543 172.16.10.200 /forum.php id=1%20and%... GET 特征防护规则 阻断 10010 10											

2 URL <http://172.16.10.200/forum.php?id=1%20and%201=1>



t Found

404 No

WEB

HTTP

WEB

“Web -> Web -> HTTP” Web HTTP Web Web

增加Web防护策略

基本配置 错误页面配置 重定向配置 会话管理 数据压缩

名称 * Cookies_test

服务器 Cookies_test

Web主机 ? --请输入或选择--

源IP 空

Web防护模板 Cookies_test

访问日志 关闭

优先级 * ? 1

启用 ☒

(0~10000)

保存 取消

弱密码检测规则 空

保存 取消

30

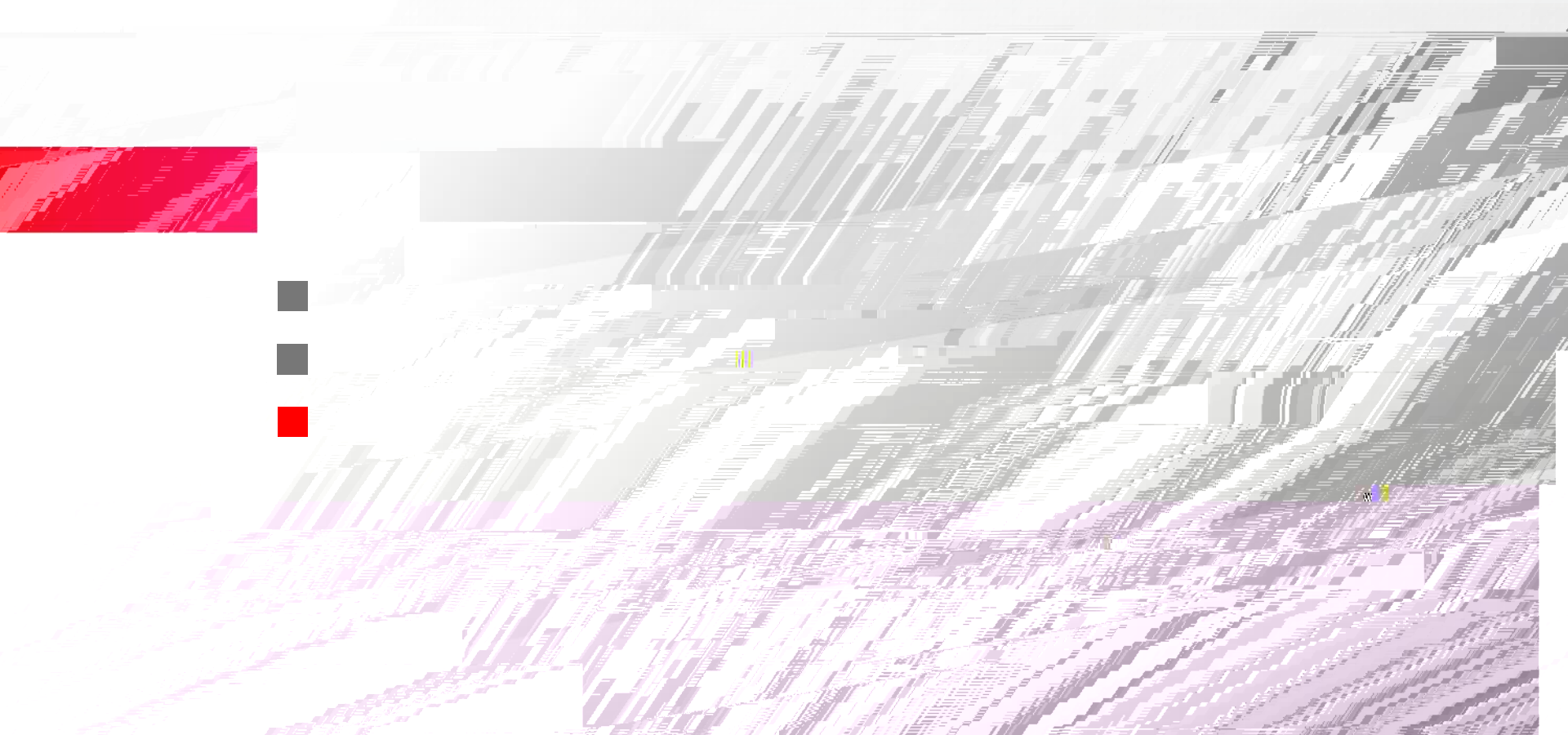
WEB

404



“ -> ”

+ 攻击日志										条件	清空
每页显示 15											
☐	时间	源IP	源端口	站点域名/IP	目标URL	状态	方法	攻击类型	处理动作		
☐	2017-12-26 11:23:32	172.16.10.15	8080	172.16.10.200		200	GET	HTTP GET request	成功		



WG
WG

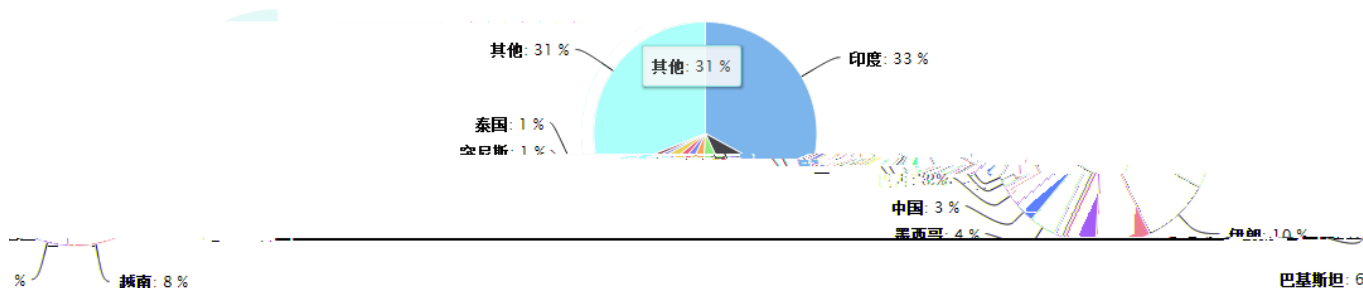
WG
IP

WG

IP

+ 安全情报IP数量统计

安全情报IP数量统计



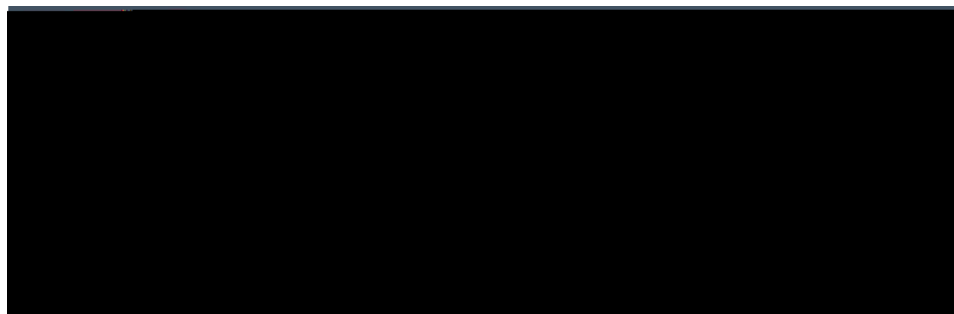
		IP数量	百分比	国家
		367639	3%	中国
961812		10%	伊朗	
2529948	31%		其他	
3168614	33%		印度	
431439	4%		墨西哥	
624148	6%	巴基斯坦		
289135	3%	巴西		
178339	1%	泰国		
188634	1%	突尼斯		
811424	8%	越南		

1

“

->

”



2



3

4

Windows

1

+ 安全情报中心规则										增
15										
低级	开启	开启	☐	邮件	僵尸网络 Windows漏洞利用 扫描器 ...	通过				
低级	开启	开启	☐	图书馆	僵尸网络 Windows漏洞利用 扫描器 ...	通过				

2

编辑安全情报中心规则

名称 * 学校主页

服务器 学校主页

检测类型 ☒ 僵尸网络 ☒ Windows漏洞利用

严重级别 低级

告警设置 ☐ 邮件

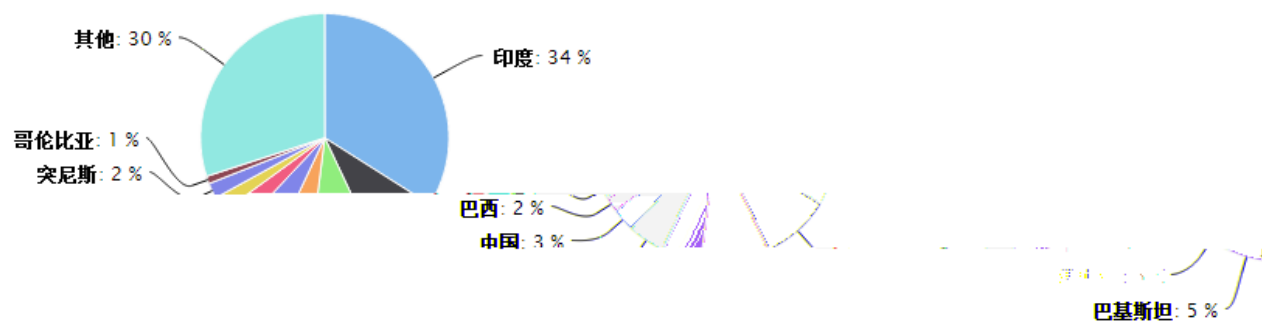
日志 ☒

启用 ☒

保存 取消

+ 安全情报活跃度统计

安全情报活跃度统计



	活跃程度	百分比	国家
	177299	3%	中国
	555030	9%	伊朗
	1469464	30%	其他
	1980738	34%	印度
	5%	巴基斯坦	346015
	2%	巴西	163145
	2%	突尼斯	118150
	9%	越南	572187

www.ruijie.com.cn

www.ruijie.com.cn/service.aspx

bbs.ruijie.com.cn

webchat.ruijie.com.cn

4008-111-000