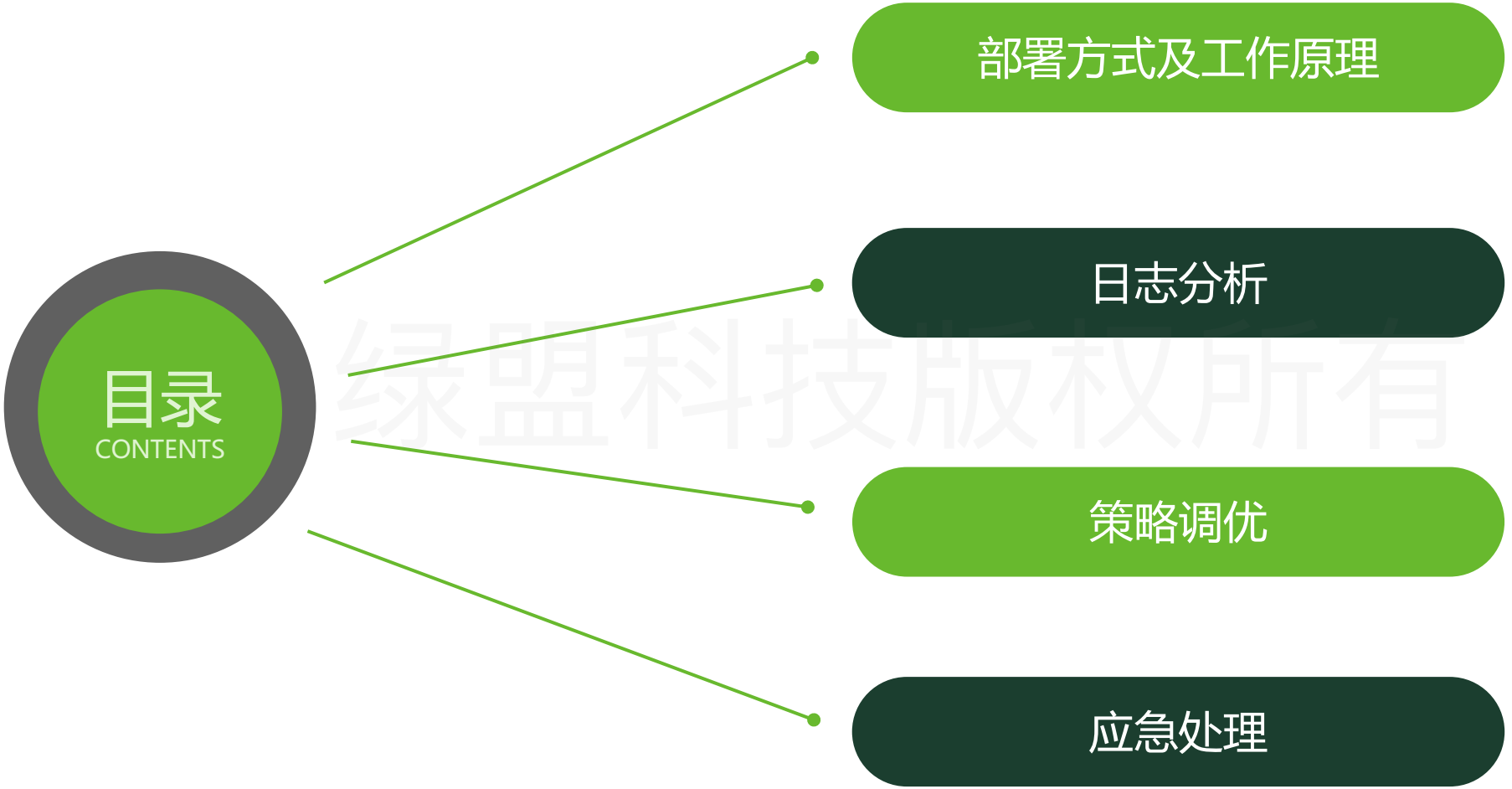
WAF使用介绍及日志分析

2019护网专项培训

NSFOCUS

目录

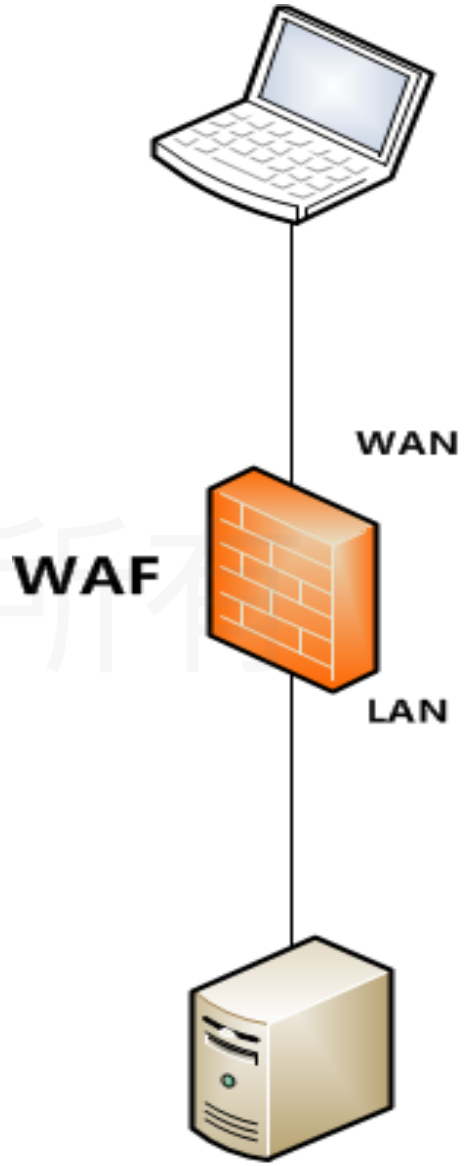


01

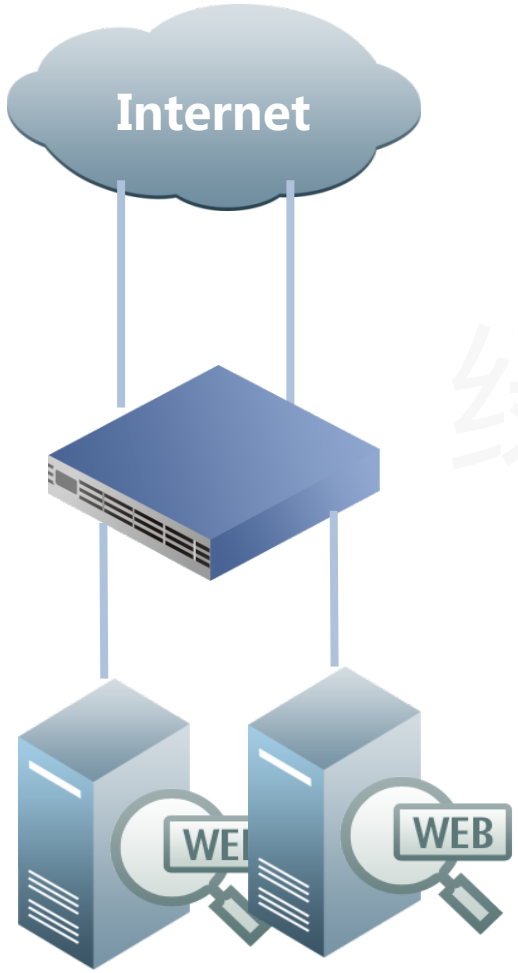
部署方式及工作原理

透明部署

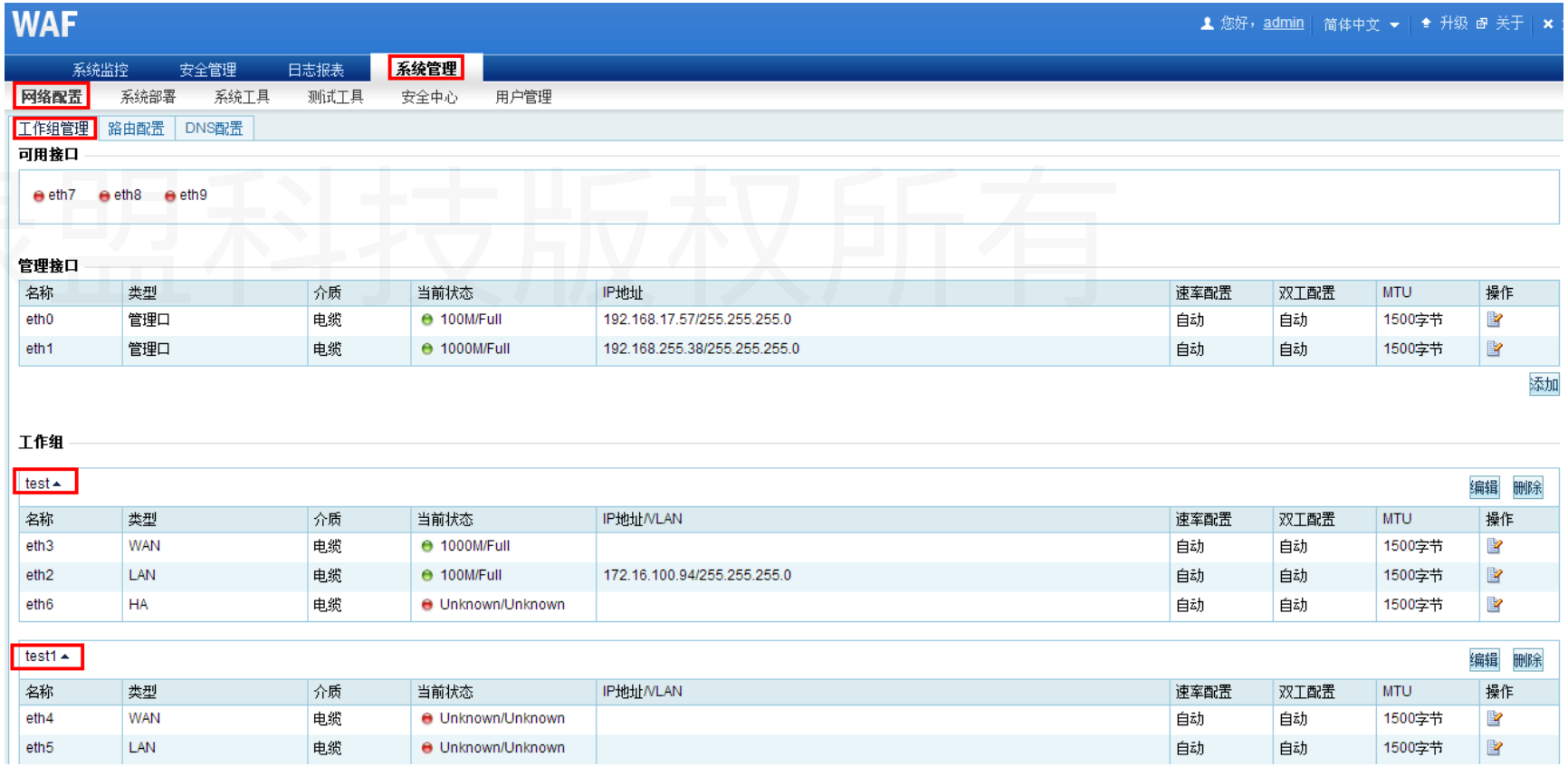
- 应用场景：
- 不改动原有网络拓扑
- 不增加网络设备的接口
- WAF关机不影响服务器的访问



多路串联部署



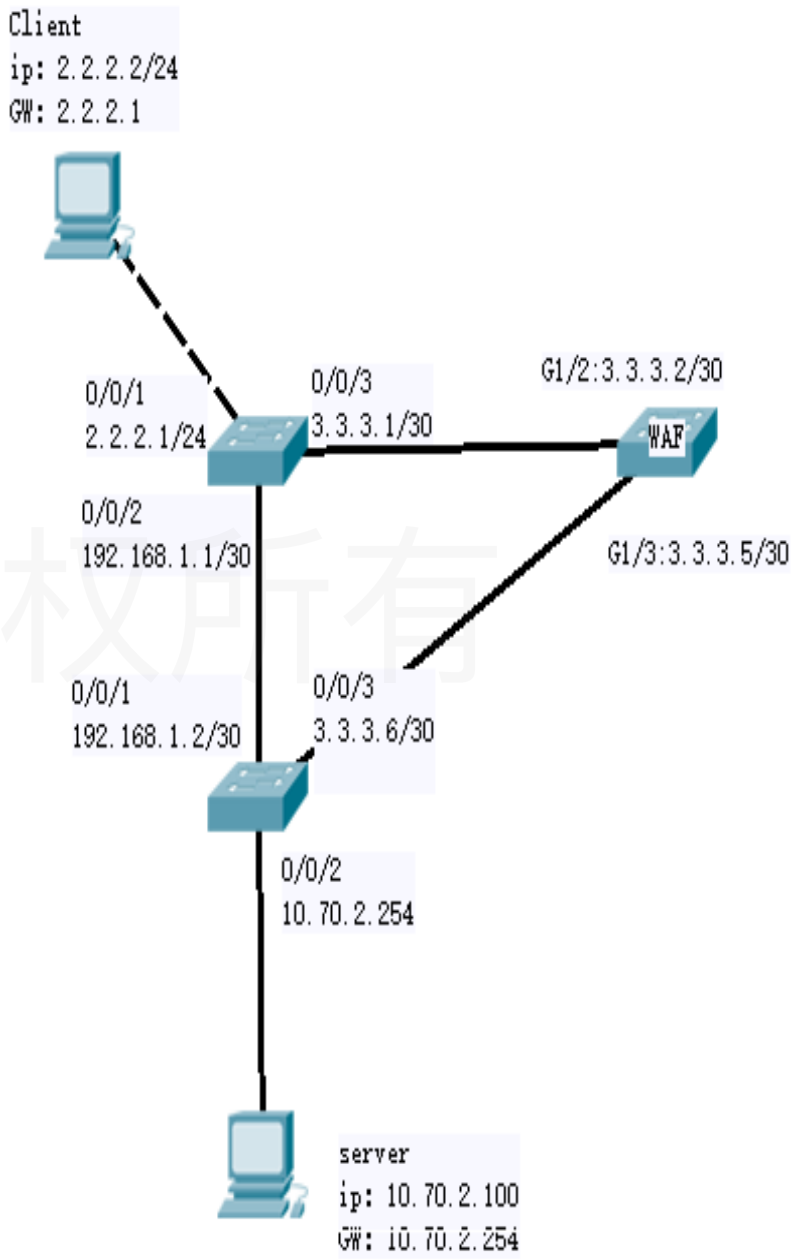
多路串联部署：
选择正确的接口，创建多个工作组



半透明部署

- 牵引：
  静态路由牵引

- 回注：
  二层回注
  跨接回注
  PBR回注



不透明部署

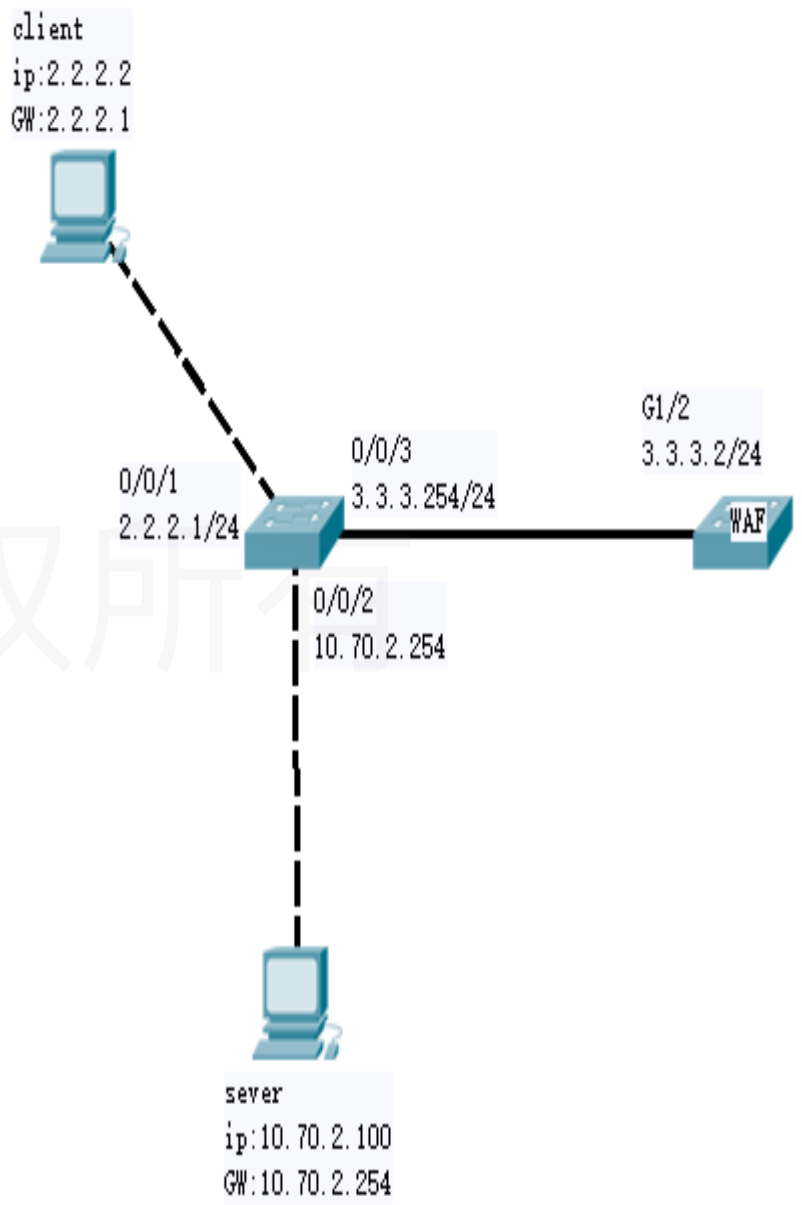
- 应用场景：

  不希望把WEB服务器暴露在公网

- 特点：

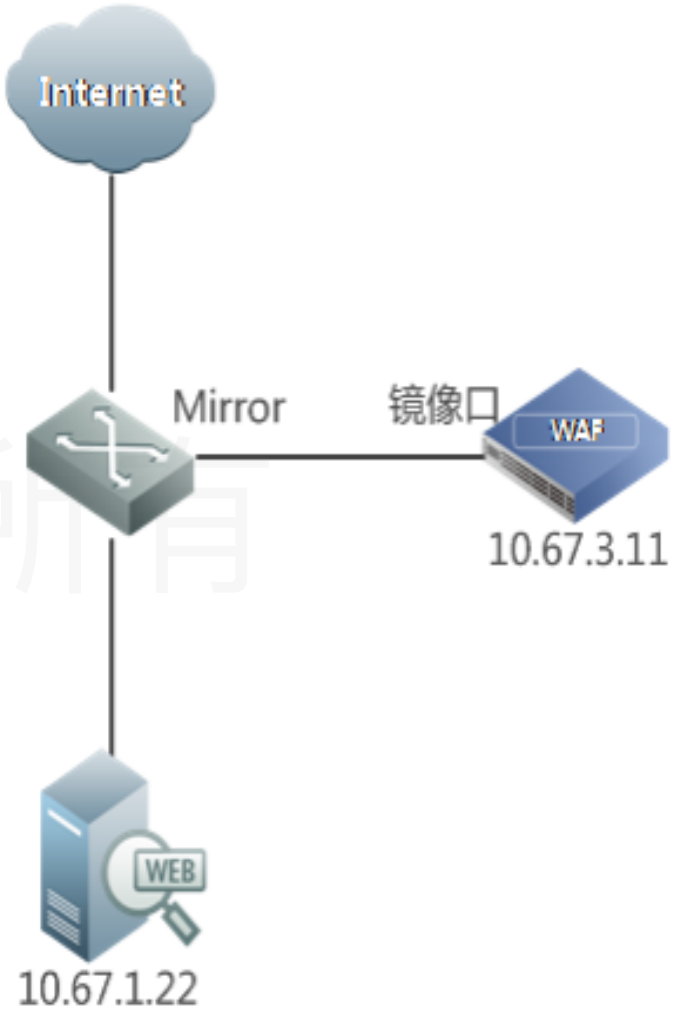
  客户端与服务器互相均不可见

  只转发代理策略匹配的HTTP流量



镜像模式

- 应用场景：
  - 只需要检测是否被攻击
  - 不需要防护

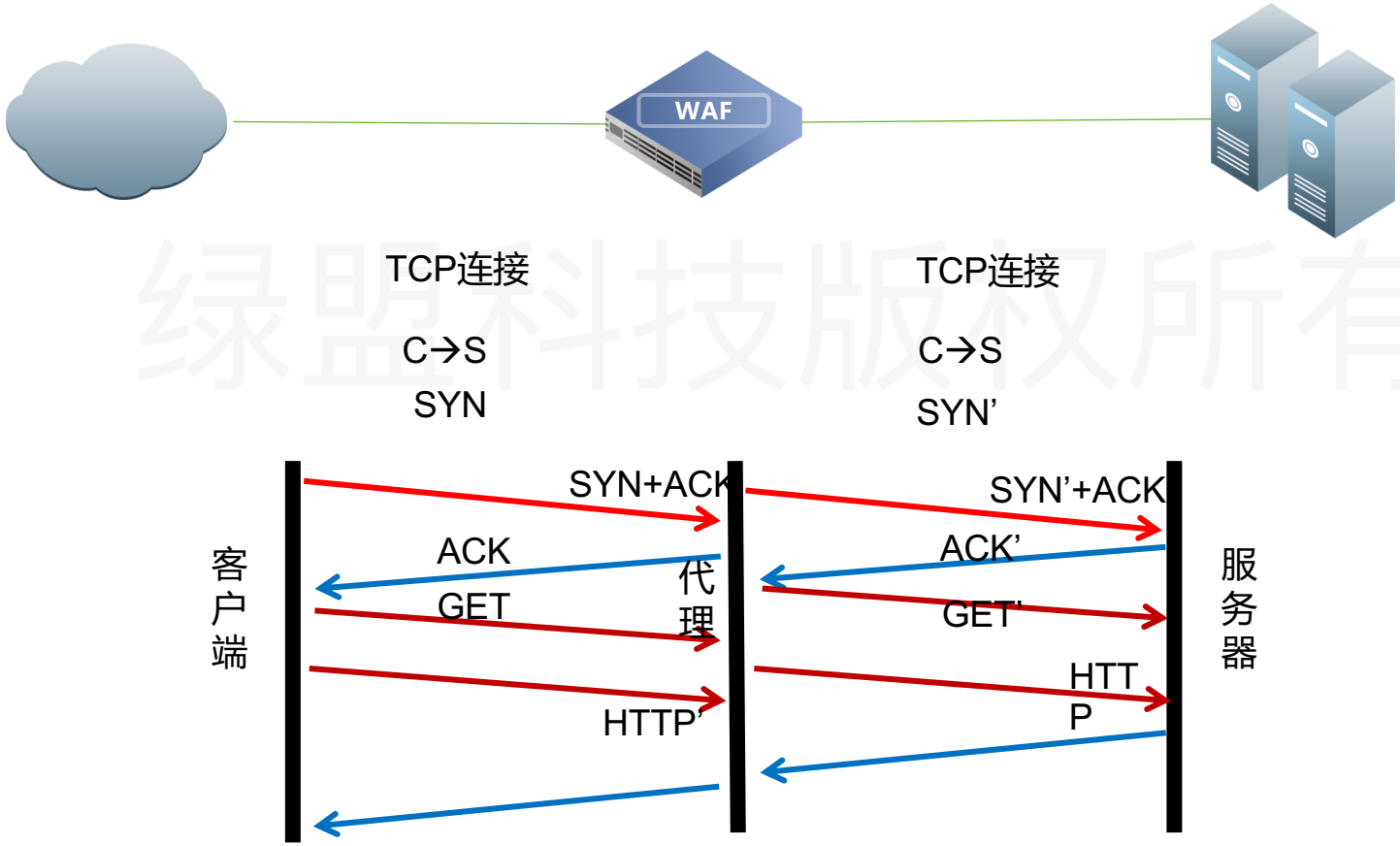


部署方式比较

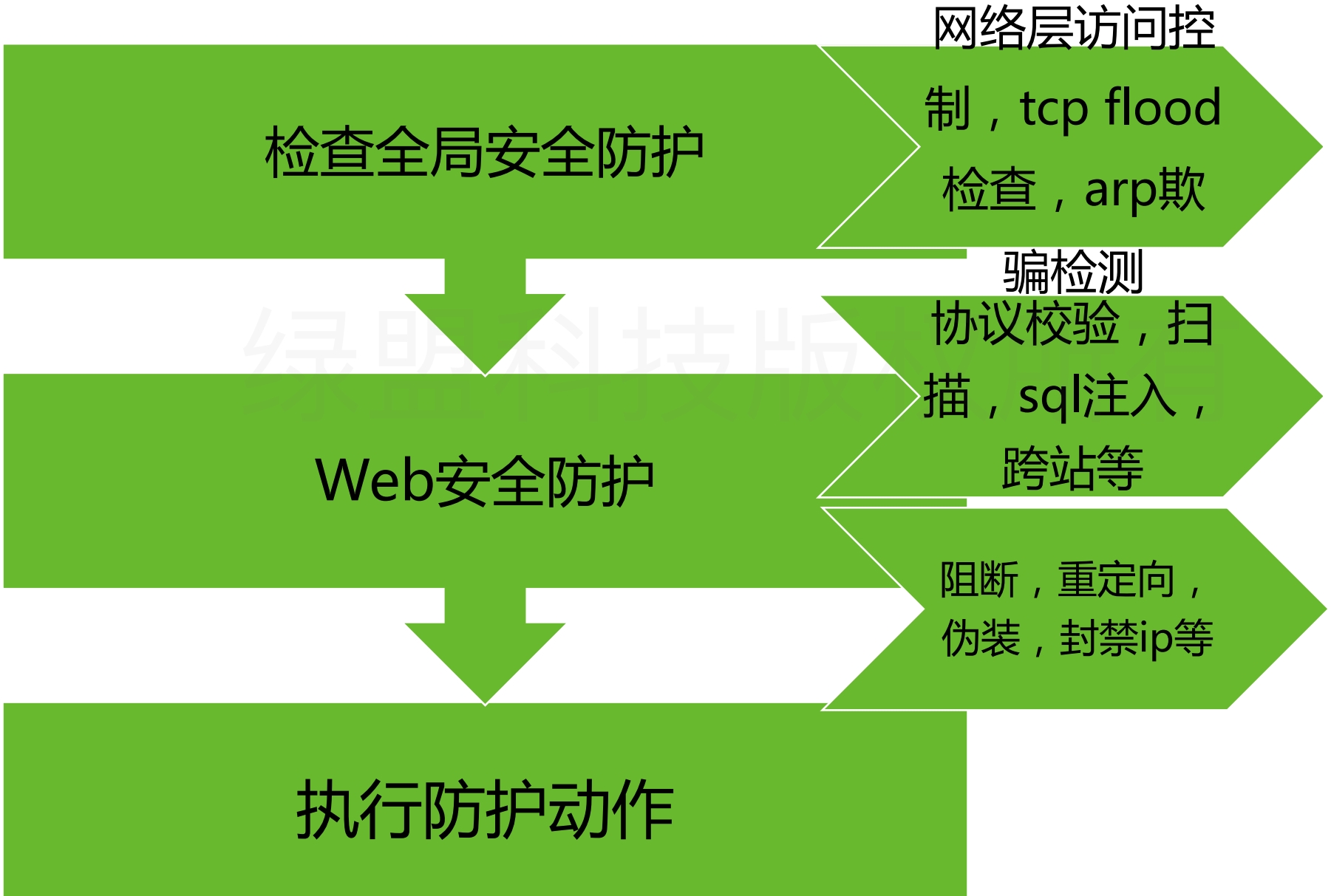
区别 / 部署方式	优势	劣势
串联部署	部署简单，不需要客户网络做较大的改变	WAF设备自身出现的问题可能会影响客户网络。 所有的流量都会经过WAF，增大了WAF的负载
旁路部署	系统资源利用率高，无需转发非Web服务器的流量 无网络单点故障	部署复杂，需要配置二层或三层流量牵引
反向代理部署	部署简单 系统资源利用率高，无需处理非HTTP流量 无网络单点故障	对客户的业务逻辑影响较大，需要更换对外业务IP或服务器IP及DNS解析。 客户端与服务器端通讯不透明
镜像监听	无需改变客户网络拓扑 不影响客户业务运行 吞吐量大	只能检测服务是否被攻击，不能对客户的业务安全进行防护。

WAF工作机制

以串联为例，基于反向代理架构的透明模式



WAF防护过程



02

日志分析

日志分析

- 误报的概念
- 常见web攻击
- 筛选过滤

常见WEB攻击

- **sql注入，跨站脚本攻击（XSS），远程文件包含，命令注入，文件非法上传，暴力破解等**

1、规则描述

查看WAF的规则描述，了解攻击常见关键字

2、看书

《 HTTP权威指南》、《web安全深度剖析》、《白帽子讲web安全》

3、实验

绿盟实训平台、Webgoat、DVWA、OWASP

常见攻击语句

- **xss**

<script>alert('xss')</script>

<img src="" onerror=alert("xss")>

<img src="" javascript:alert("xss")>

- **sql注入**

or ‘1’ = ‘1、and 1 = 1 、Ordey by、union select、concat()、group_concat()、sleep()等

select schema_name from information_schema.schemata

union select 1,concat(id,0x3a,name,0x3a,passwd),3,4,5 from users

- **路径穿越**

../../../../etc/passwd

常见攻击语句

- **php一句话木马**

```
<?php @eval($_POST[value]);?>

<?php assert($_POST[qazw]);?>

<?php $a = str_replace(""vbnm"","""","asvbnmsert""); $a($_POST[qazw]);?>
```

- **asp一句话木马**

```
<%eval request("MH")%>

<%execute request("MH")%>
```

常见攻击语句

- **jsp一句话木马**

```
<%Runtime.getRuntime().exec(request.getParameter("i"));%>

<%if(request.getParameter("f")!=null)(newjava.io.FileOutputStream(application.getReal
Path("\")+request.getParameter("f"))).write(request.getParameter("t").getBytes());%>
```

恶意攻击判断

确认匹配关键词

查看规则描述

是否

部分防护举例

内置协议校验

- 检测报文是否符合RFC规范
- 检查内容是请求方式，头部字段合规情况等
- 6061版本可自定义放过项目

Sql注入

- 检测访问输入的参数，进行关键字和特征匹配，如sql语句，闭合构
- 参数中检测匹配到对应特征或者关键字（规则需已勾选启用）
- 匹配中规则后执行对应策略动作进行防护，产生告警

XSS

- 检查用户提交的http数据字段
- 检查到异常的script标签闭合，跨站语句特征（规则需启用）
- 执行对应防护策略进行防护，产生告警

误报判断

确认匹配关键词

误报判断

点击匹配规则，查看规则具体描述

互动

- 是否误报？

筛选过滤

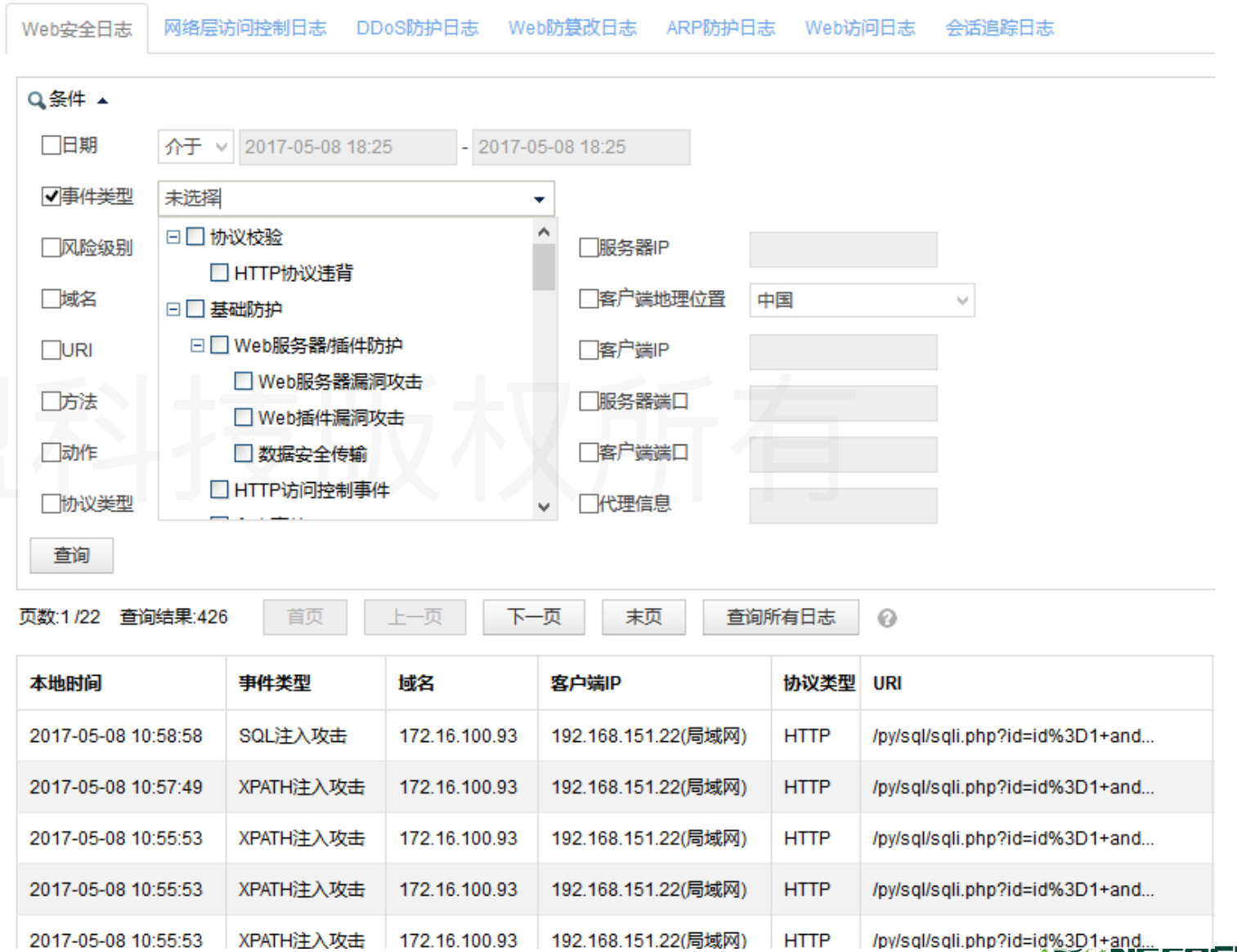
- 通过协议过滤

筛选过滤

- 通过URI过滤

筛选过滤

- 通过告警类型过滤



03

策略优化

策略优化

1资产登记

- IP和端口
- 域名
- 开发语言
- 中间件类型
- 系统类型
- 数据库类型

2创建站点

- 向导模式
- 补充策略
- 准确度高

3日志

- 仅
- 解
- 一

策略优化

4规则调优

- 日志分析
- 误报排除
- 添加例外

5开启阻断

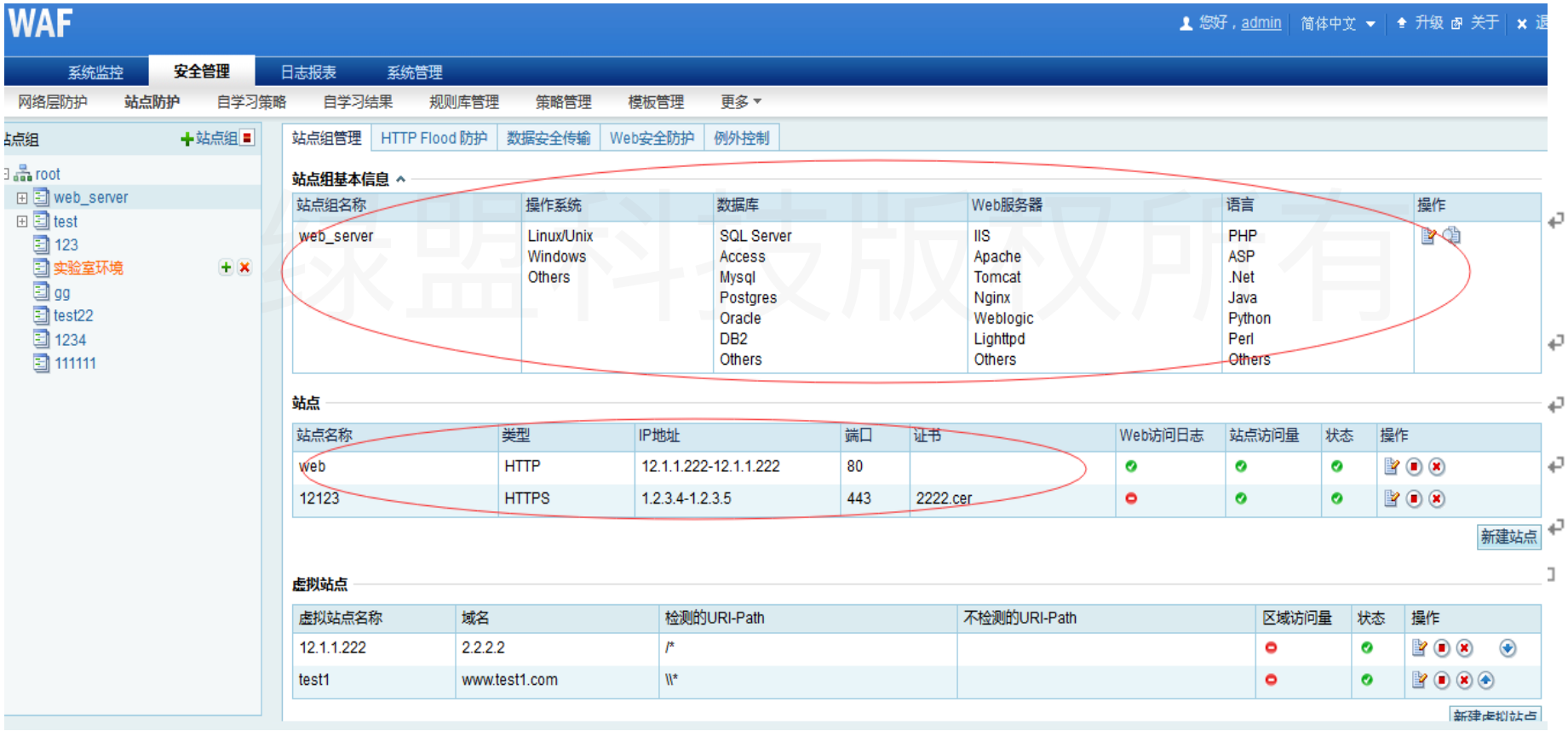
- 逐步开启

6试运

- 观
- 误

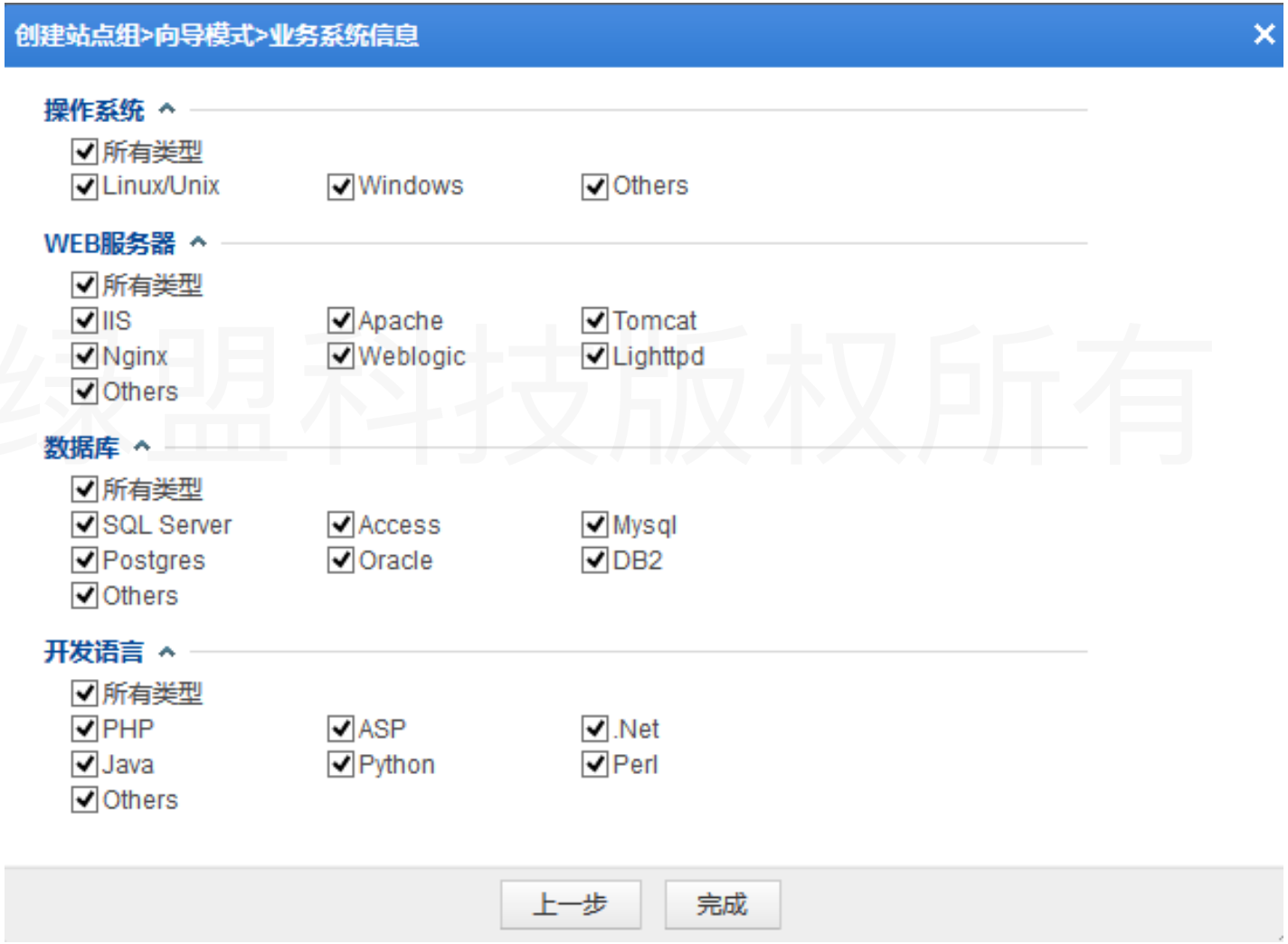
策略优化

资产登记


WAF
您好，admin
简体中文
升级
关于
系统监控
安全管理
日志报表
系统管理
网络层防护
站点防护
自学习策略
自学习结果
规则库管理
策略管理
模板管理
更多
站点组
站点组
root
web_server
test
123
实验室环境
gg
test22
1234
111111
站点组管理
HTTP Flood 防护
数据安全传输
Web安全防护
例外控制
站点组基本信息
站点组名称
操作系统
数据库
Web服务器
语言
操作
web_server
Linux/Unix
Windows
Others
SQL Server
Access
Mysql
Postgres
Oracle
DB2
Others
IIS
Apache
Tomcat
Nginx
Weblogic
Lighttpd
Others
PHP
ASP
.Net
Java
Python
Perl
Others
站点
站点名称
类型
IP地址
端口
证书
Web访问日志
站点访问量
状态
操作
web
HTTP
12.1.1.222-12.1.1.222
80
12123
HTTPS
1.2.3.4-1.2.3.5
443
2222.cer
新建站点
虚拟站点
虚拟站点名称
域名
检测的URI-Path
不检测的URI-Path
区域访问量
状态
操作
12.1.1.222
2.2.2.2
/*
test1
www.test1.com
*

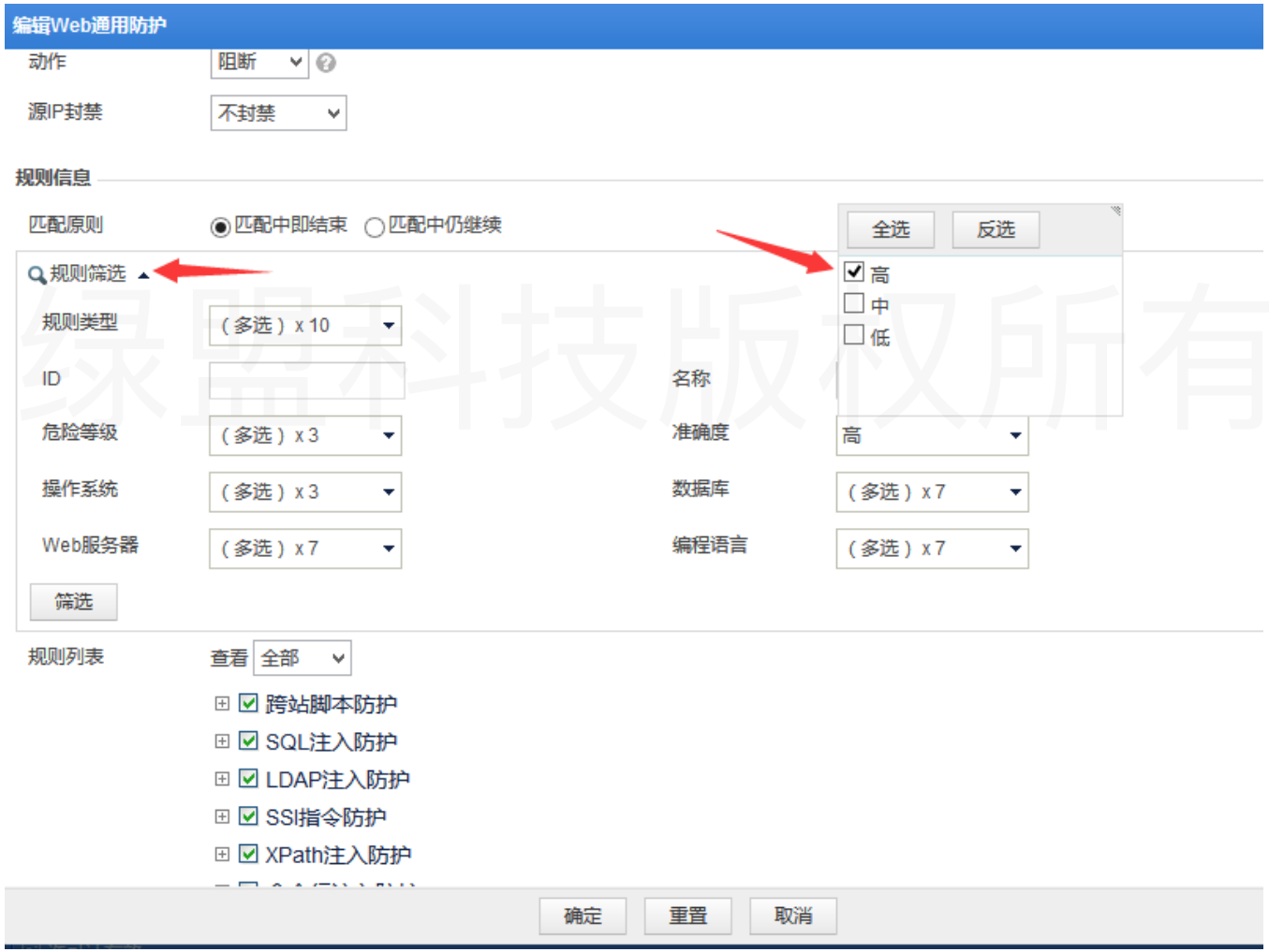
策略优化

向导模式



策略优化

- 仅选择准确度高的规则



策略优化

策略补充

策略优化

- 开启一键接受，解码放过，高级防护策略动作为接受，开始日志收集

案例分享

- 日志分析出误报后，进行调优

本地时间	事件类型	告警级别	域名	协议类型	URI	方法	匹配策略	匹配规则	动作	IP封禁	例外控制	详情
2015-09-10 07:39:15	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:39:15	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:39:14	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:39:14	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:39:14	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:39:13	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:39:13	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:39:13	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:50	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:50	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:50	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:50	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:50	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:49	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:49	Web服务器漏洞攻击	高	www[illegible]cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:49	Web服务器漏洞攻击	高	www[illegible].cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:38:49	Web服务器漏洞攻击	高	www[illegible].cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:37:50	Web服务器漏洞攻击	高	www.[illegible].cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:37:50	Web服务器漏洞攻击	高	www.[illegible].cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	
2015-09-10 07:37:50	Web服务器漏洞攻击	高	www.[illegible].cn	HTTP	/jwzx/jywh../shsy/201407/W0201...	GET	default_medium-1	tomcat_dir_traver_vulner	阻断	不启用	添加到例外策略	

策略优化

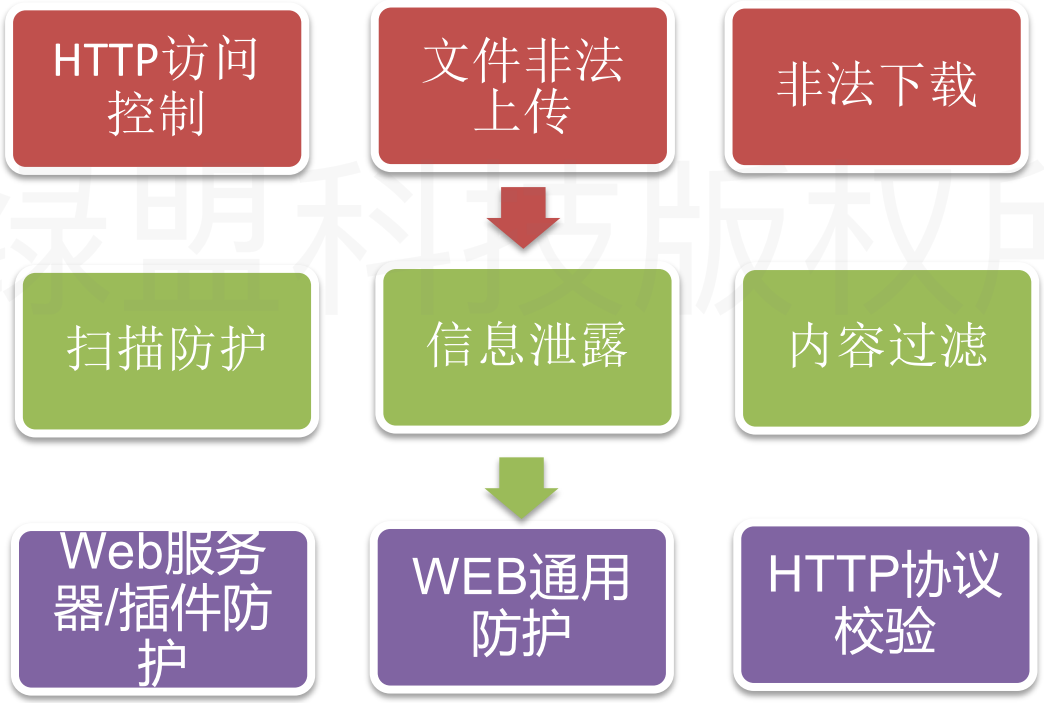
- 日志分析出误报后，进行调优

页数:12 /19　查询结果:370　首页　上一页　下一页　末页　查询所有日志

本地时间	事件类型	域名	客户端IP	协议类型	URI	风险级别	方法	匹配策略	匹配规则	动作	IP封禁	操作
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/WebGoat/attack?Screen=186&men...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/WebGoat/attack?Screen=186&men...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/WebGoat/attack?Screen=186&men...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/inc/checkout1%2dFR.php?includ...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/admin/modules/modules/forum/a...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/obj/profil.class.php?path%5fo...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/gen/obj/profil.class.php?path...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/kb.php?path%5ffaqe=http://www...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/plugins/DPGguestbook/guestboo...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/template/calm/top.php?menu=ht...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/template/babyweb/index.php?te...		GET	tt1		伪装	不启用	
2017-05-03 11:45:25	服务器信息泄露	172.16.100.93	192.168.151.22(局域网)	HTTP	/mail.inc.php?root=http://www....		GET	tt1		伪装	不启用	

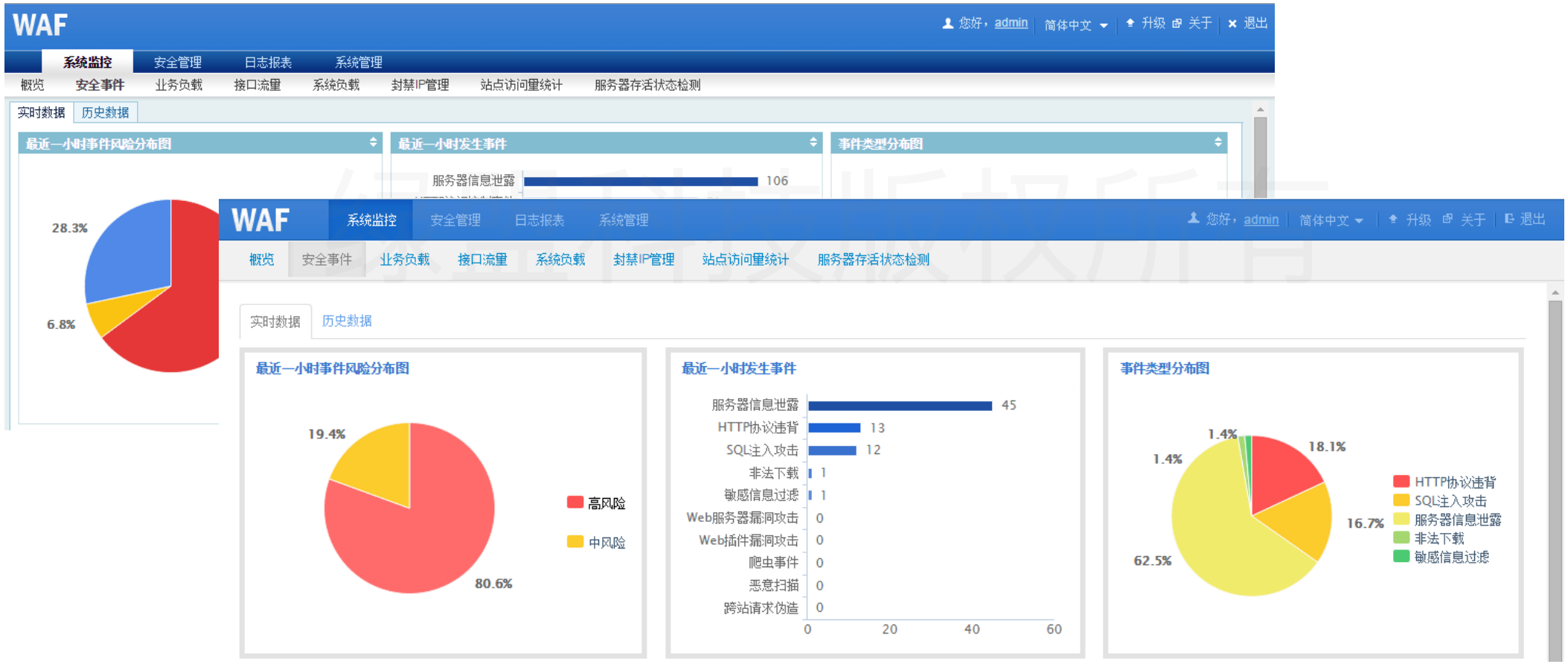
策略优化

- 逐步开启阻断，按照误报率从低到高的顺序



策略优化

- 调优前后告警数量对比



03

应急处理

应急处理

- 误防处理
- 漏防处理
- 业务受影响
- 界面报错
- WAF自身故障

误防处理

日志分析 → 加例外策略or调整对应防护规则 → 验证问题解决

漏防处理

攻击绕过？ → 确认攻击类型，特征 → 调整策略勾选上对应规则 → 验证防护效果 → 防护成功

对于已有规则无法防护？新爆出漏洞？ → 直接打客服热线跟技术支持确认

业务受影响

- 所有业务受影响？单个业务受影响？

处理方法： 排除策略影响（空策略测试）

停止站点防护测试？转发模式测试？bypass测试？

抓包很重要！

界面报错

- 登录报错？首页及日志查询报错？功能页面报错？

WAF自身故障

- 设备无法登陆？443不通？

可能原因：apache异常，端口没启用，

处理方法： 第一时间检查是否有影响业务；可尝试串口重启apache。

THANKS!

NSFOCUS Information Technology Co., Ltd

地址: 北京市海淀区北洼路4号益泰大厦3层

电话: 010-68438880

邮编: 100089