



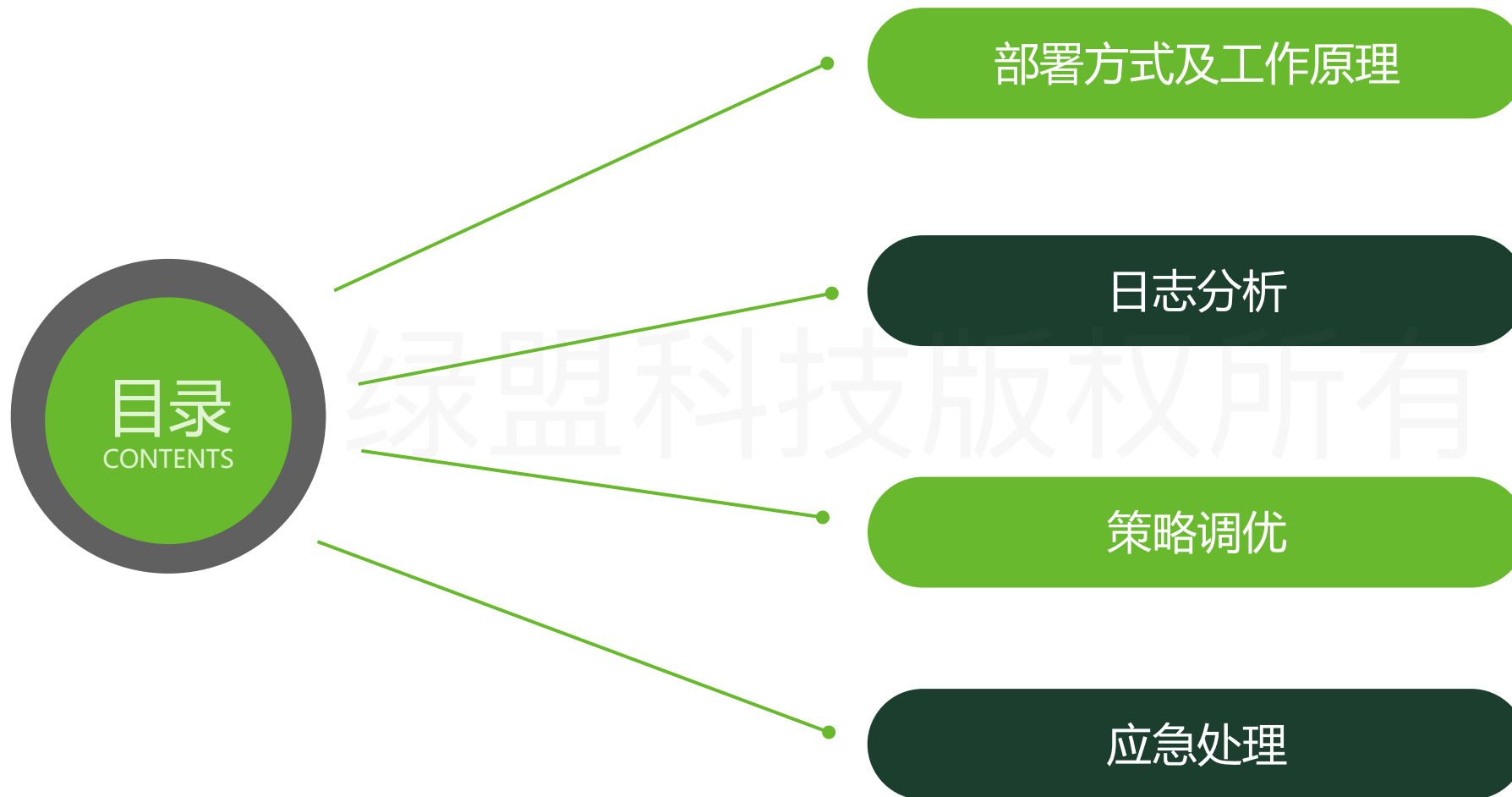
# WAF使用介绍及日志分析

绿盟科技版权所有

2019护网专项培训



# 目录



01

# 部署方式及工作原理

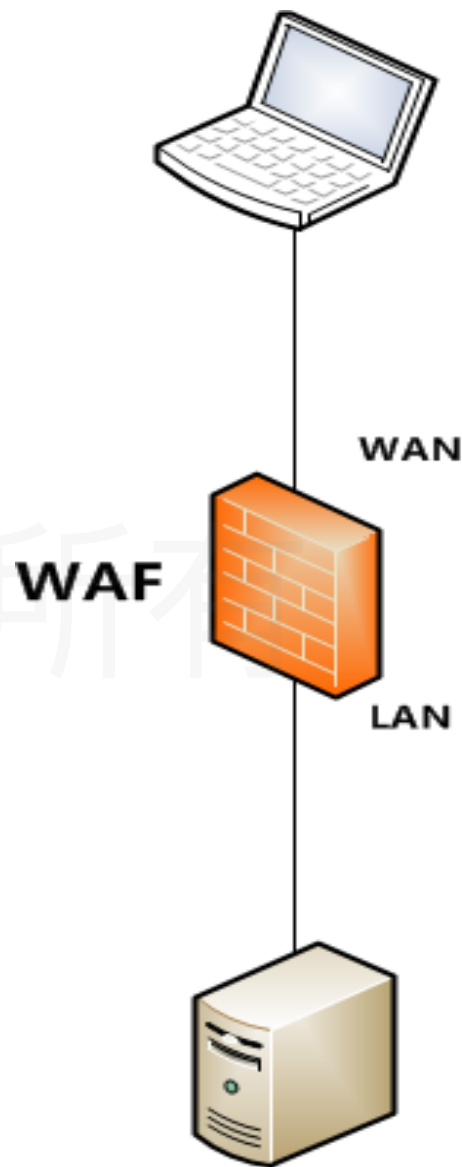


串联部署

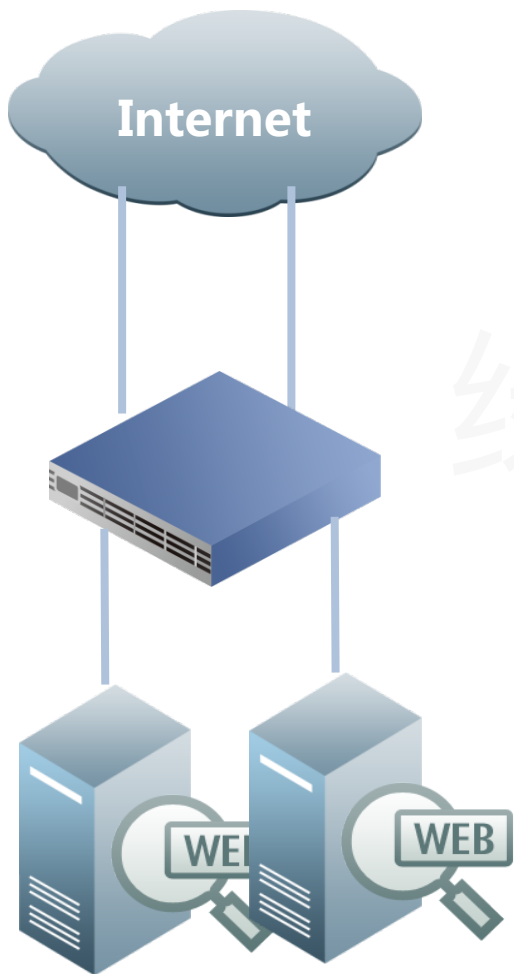


## 透明部署

- 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

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**

网络配置 系统部署 系统工具 测试工具 安全中心 用户管理

工作组管理 路由配置 DNS配置

可用接口

eth7 eth8 eth9

管理接口

名称	类型	介质	当前状态	IP地址	速率配置	双工配置	MTU	操作
eth0	管理口	电缆	100M/Full	192.168.17.57/255.255.255.0	自动	自动	1500字节	
eth1	管理口	电缆	1000M/Full	192.168.255.38/255.255.255.0	自动	自动	1500字节	

添加

工作组

test

名称	类型	介质	当前状态	IP地址/VLAN	速率配置	双工配置	MTU	操作
eth3	WAN	电缆	1000M/Full		自动	自动	1500字节	
eth2	LAN	电缆	100M/Full	172.16.100.94/255.255.255.0	自动	自动	1500字节	
eth6	HA	电缆	Unknown/Unknown		自动	自动	1500字节	

编辑 删除

test1

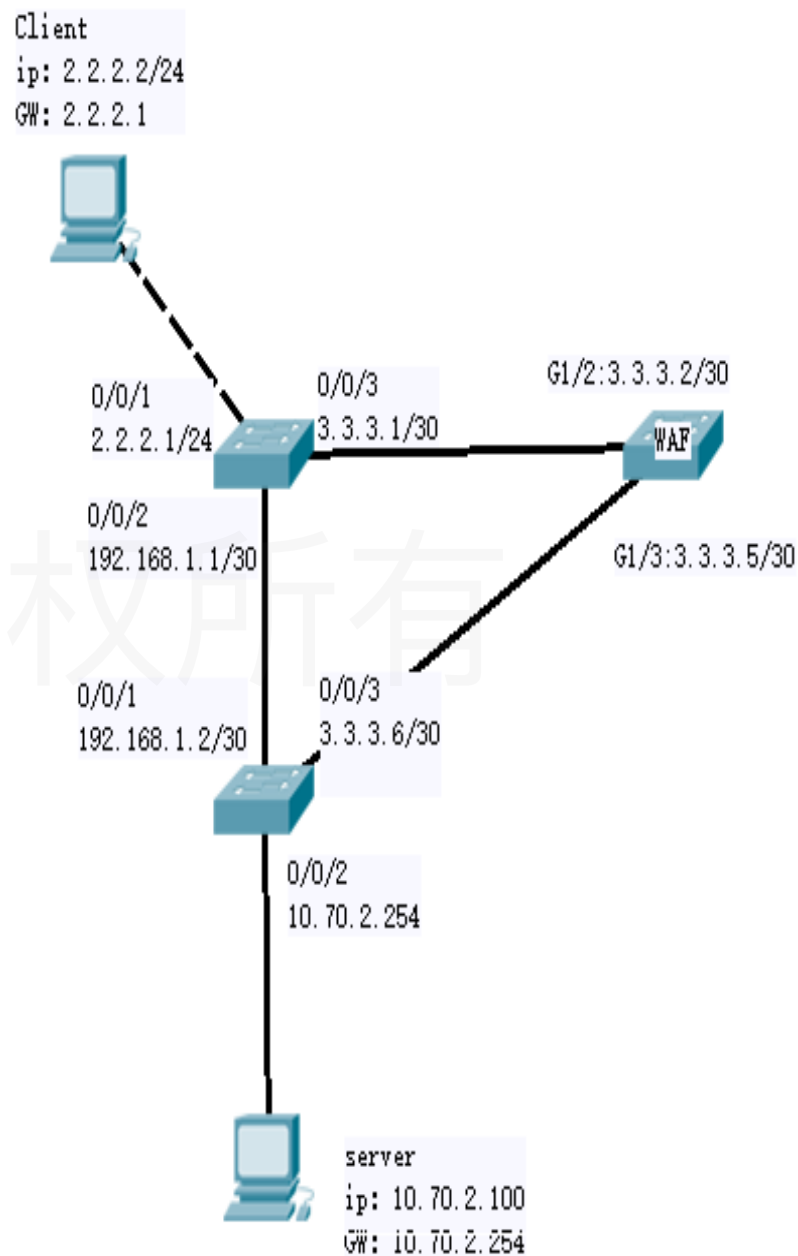
名称	类型	介质	当前状态	IP地址/VLAN	速率配置	双工配置	MTU	操作
eth4	WAN	电缆	Unknown/Unknown		自动	自动	1500字节	
eth5	LAN	电缆	Unknown/Unknown		自动	自动	1500字节	

编辑 删除

## 旁路部署

# 半透明部署

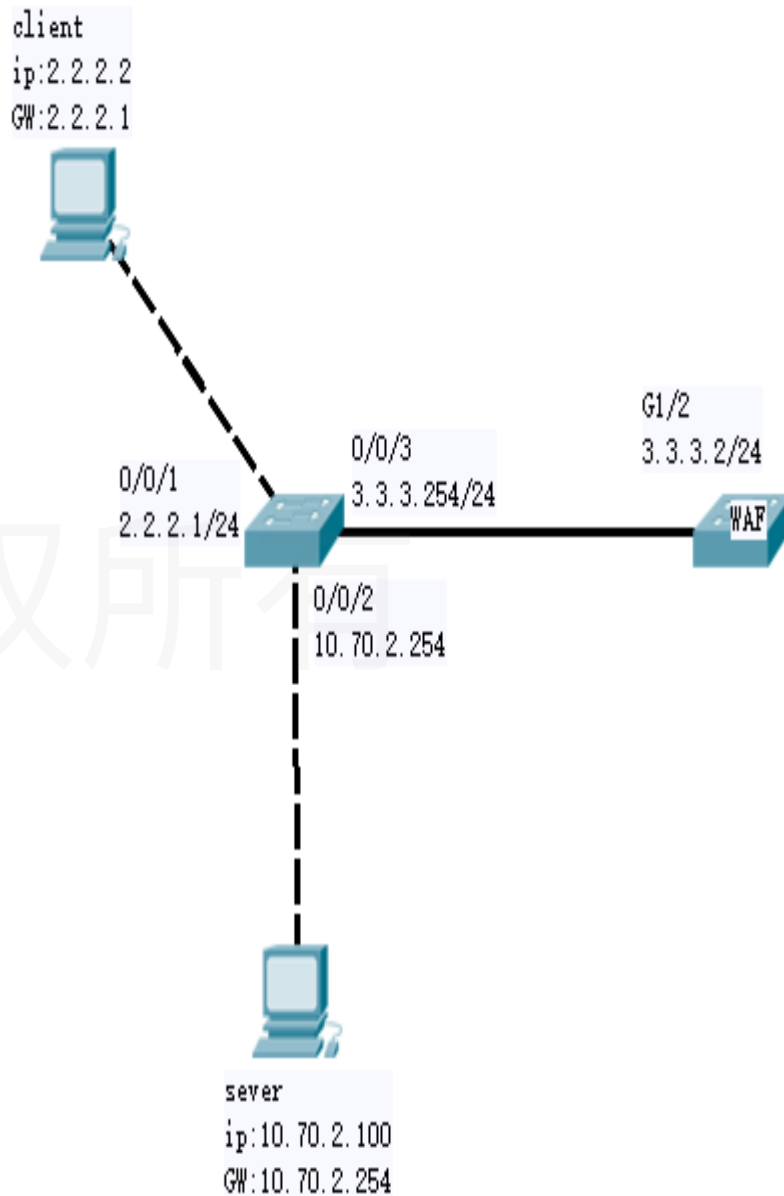
- 牵引：  
静态路由牵引
- 回注：  
二层回注  
跨接回注  
PBR回注



## 反向代理部署

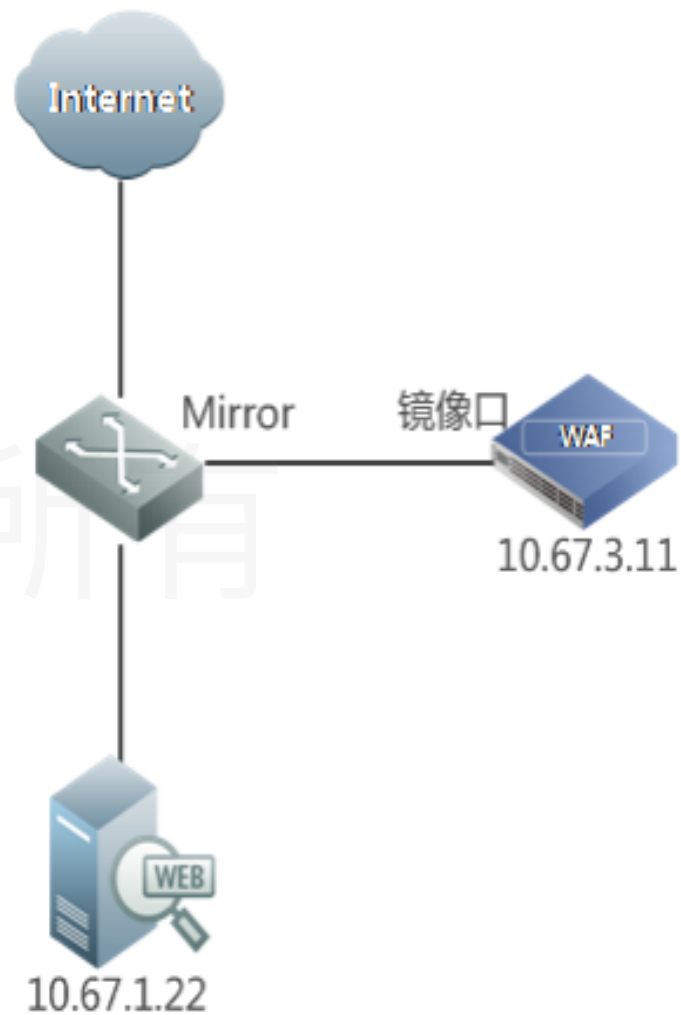
### 不透明部署

- 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



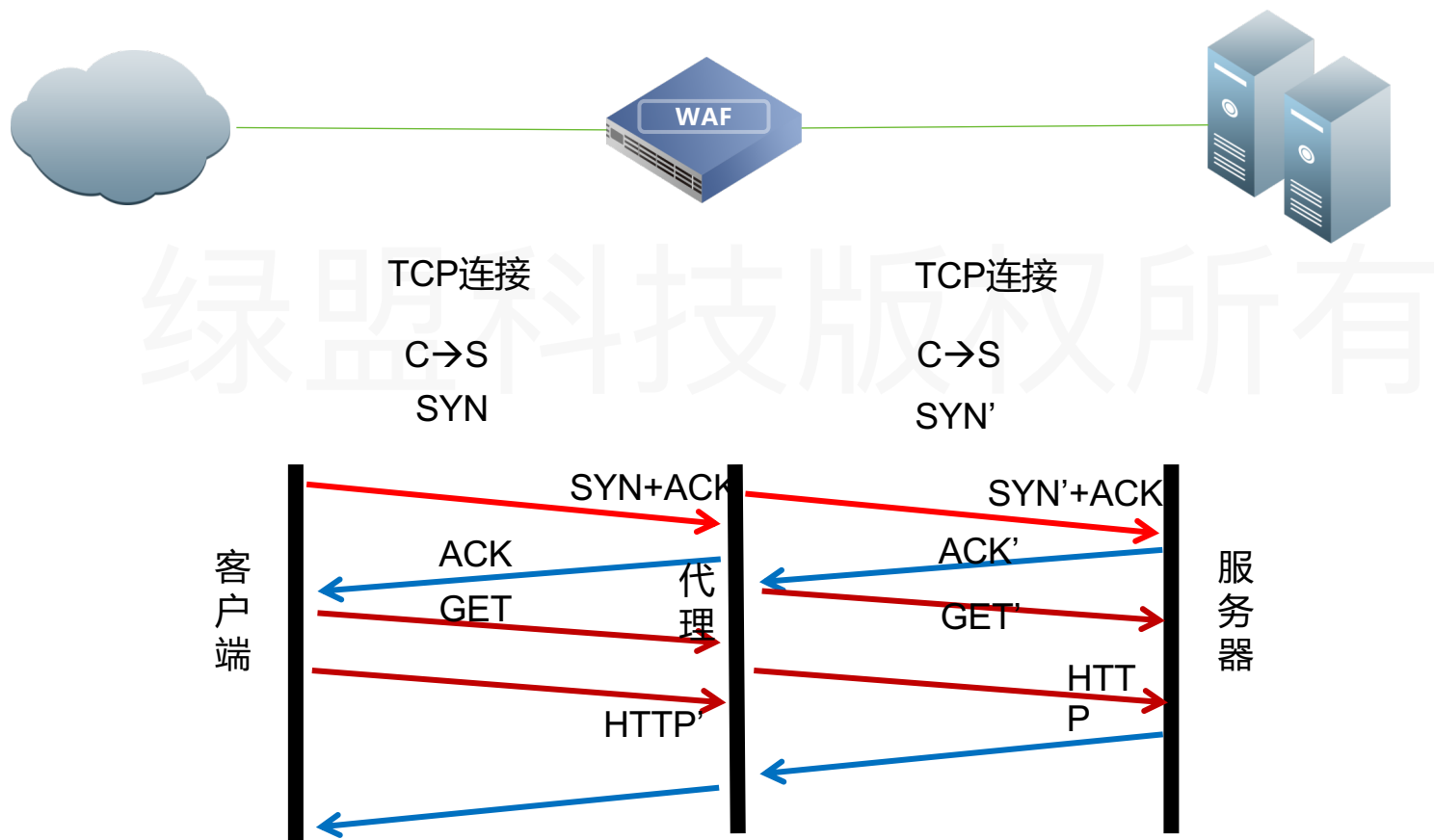


## 部署方式比较

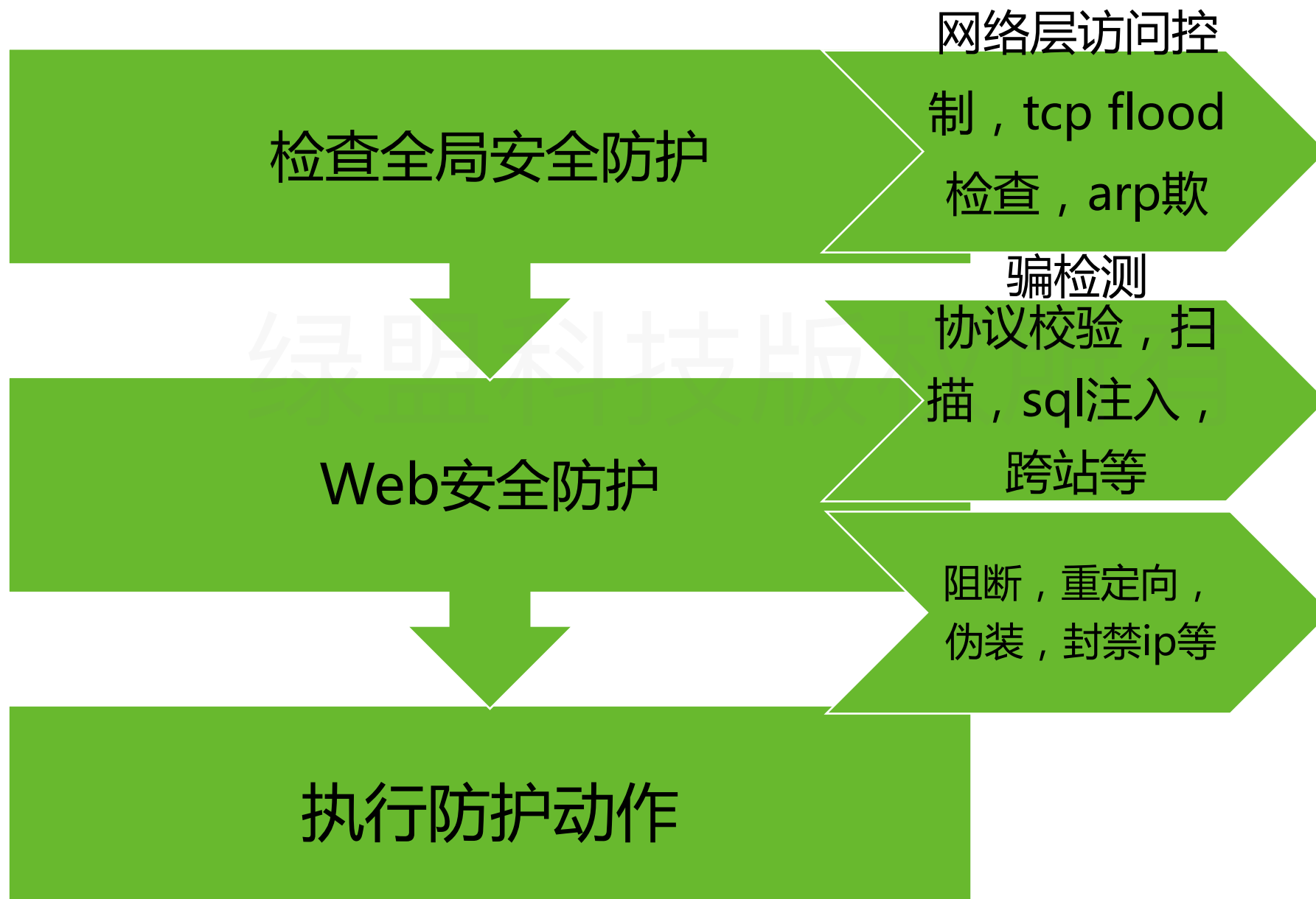
部署方式 \ 区别	优势	劣势
串联部署	部署简单，不需要客户网络做较大的改变	WAF设备自身出现的问题可能会影响客户网络。 所有的流量都会经过WAF，增大了WAF的负载
旁路部署	系统资源利用率高，无需转发非Web服务器的流量 无网络单点故障	部署复杂，需要配置二层或三层流量牵引
反向代理部署	部署简单 系统资源利用率高，无需处理非HTTP流量 无网络单点故障	对客户的业务逻辑影响较大，需要更换对外业务IP或服务器IP及DNS解析。 客户端与服务器端通讯不透明
镜像监听	无需改变客户网络拓扑 不影响客户业务运行 吞吐量	只能检测服务是否被攻击，不能对客户业务安全进行防护。

## 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

绿盟科技版权所有

## ▶▶ 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.getRealPath("\")+request.getParameter("f"))).write(request.getParameter("t").getBytes());%>
```

绿盟科技版权所有



## 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，闭合构造
- 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

### 事件详情

匹配特征	Param_list:message=<IMG DYNSRC="javascript:alert('XSS')">
代理信息	
HTTP请求或者响应信息	<p><a href="#">查看原始HTTP信息</a> <a href="#">下载HTTP信息</a></p> <p>POST /WebGoat/attack?Screen=2634&amp;menu=900 HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-us,en;q=0.5 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Authorization: Basic Z3Vlc3Q6Z3Vlc3Q= Content-Type: application/x-www-form-urlencoded Pragma: no-cache Cache-Control: no-cache Referer: http://172.16.100.93/WebGoat/attack?Screen=2634&amp;menu=900 Content-Length: 100 Host: 172.16.100.93 Connection: Keep-Alive User-Agent: Apache-HttpClient/4.1.1 (java 1.5)</p> <p>title=&amp;message=&lt;IMG DYNSRC="javascript:alert('XSS')"&gt;&amp;field1=111 &amp;SUBMIT=Purchase</p>

关闭

绿盟科技版权所有

## 误报判断

点击匹配规则，  
查看规则具体描述

事件详情 ▾ 详细信息

	准确度	⚠
影响范围	操作系统	所有操作系统
	WEB服务器	所有WEB服务器
	数据库	所有数据库
	编程语言	所有系统语言
详细说明	CVE编号：N/A 危害描述：网站对用户提交的数据未作img标签过滤时，有可能被用作xss攻击，执行js代码。该规则对get和post方式传入的http数据字段值包含img标签的数据进行过滤，发现时进行告警。 配置建议：除因正常流量中会包含img标签并已经作特殊处理等，该规则可做常规性配置	

关闭

## 互动

- 是否误报？

匹配特征	Param_list
代理信息	
HTTP请求或者响应信息	<p>查看原始</p> <p>POST /Web... Accept: text... Accept-Lang... Accept-Char... Authorization... Cache-Control... Content-Type... Content-Length... Host: 172... Connection... User-Agent...</p>

事件详情 ▾ 详细信息

影响范围	准确度	!
	操作系统	所有操作系统
	WEB服务器	所有WEB服务器
	数据库	SQL Server Postgres Oracle DB2 Others
	编程语言	所有系统语言
详细说明	CVE编号: N/A 危害描述: '*/'是大多数数据库接受的块注释方式,在攻击者构造SQL注入攻击负载时常用这一块注释符来消除因改变数据库语句的执行逻辑而带来的消极影响,因此带有这一块注释符常常是辅助成功进行SQL注入攻击的关键,该规则对参数值中包含'/*'这种情况做检测 配置建议: 严格配置该规则对参数进行SQL注入检测	

关闭

title=&message=neQRQBqOKtQ-ZzrqLSgzCmp/sK8yV9/\*g&SUBMIT  
=Submit



## 筛选过滤

- 通过协议过滤

**WAF** 系统监控 安全管理 **日志报表** 系统管理 您好, a

安全防护日志 流量控制日志 系统运行日志 安全报表 流量报表 区域访问量统计报表 PCI-DSS合规报表 日志管理配置

Web安全日志 DDoS防护日志 Web防篡改日志 Web访问日志 会话追踪日志

Q 条件 ▲

日期 介于 2017-05-03 11:06 - 2017-05-03 11:06

事件类型 未选择

风险级别 高

域名 =

URI =

方法 UNKNOWN

动作 放过

协议类型 HTTP

服务器IP

客户端地理位置 中国

客户端IP

服务器端口

客户端端口

代理信息

查询

页数: 1 / 1 查询结果: 8 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	四
2017-04-26 14:33:32	资源盗链	172.16.100.93	192.168.151.22(局域网)	HTTP	/py/upload/files/ice.jpg	!	GET	default_high_lab	



# 筛选过滤

- 通过URI过滤

安全防护日志
您好, admin

WAF

系统监控
安全管理
日志报表
系统管理

Web安全日志
日志管理配置

DDoS防护
安全防护日志
流量控制日志
系统运行日志
安全报表
流量报表
区域访问量统计报表
PCI-DSS合规报表

Web安全日志
DDoS防护日志
Web防篡改日志
Web访问日志
会话追踪日志

Q 条件 ▲

日期 介于 ▼

事件类型 未选择

风险级别 高

域名 = ▼

URI >= ▼

方法 UNKNOWN

动作 放过

协议类型 HTTP

查询

Q 条件 ▲

日期 介于 ▼ 2017-05-03 11:06 - 2017-05-03 11:06

事件类型 未选择 ▼

风险级别 高 ▼

域名 = ▼

URI >= ▼ /abc/hello.php

方法 UNKNOWN ▼

动作 放过 ▼

协议类型 HTTP ▼

查询

页数: 1/1 查询结果: 8

本地时间
2017-04-26 14:33:32

页数: 1/1 查询结果: 8
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
2017-04-26 14:33:32	资源盗链	172.16.100.93	192.168.151.22(局域网)	HTTP	/py/upload/files/ice.jpg	!	GET	default_high_lab	





## 筛选过滤

- 通过告警类型过滤

Web安全日志 | 网络层访问控制日志 | DDoS防护日志 | Web防篡改日志 | ARP防护日志 | Web访问日志 | 会话追踪日志

Q 条件 ▲

日期 介于 2017-05-08 18:25 - 2017-05-08 18:25

事件类型 未选择

风险级别

域名

URI

方法

动作

协议类型

服务器IP

客户端地理位置 中国

客户端IP

服务器端口

客户端端口

代理信息

查询

页数: 1 / 22 查询结果: 426 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
2017-05-08 10:58:58	SQL注入攻击	172.16.100.93	192.168.151.22(局域网)	HTTP	/py/sql/sqli.php?id=id%3D1+and...
2017-05-08 10:57:49	XPATH注入攻击	172.16.100.93	192.168.151.22(局域网)	HTTP	/py/sql/sqli.php?id=id%3D1+and...
2017-05-08 10:55:53	XPATH注入攻击	172.16.100.93	192.168.151.22(局域网)	HTTP	/py/sql/sqli.php?id=id%3D1+and...
2017-05-08 10:55:53	XPATH注入攻击	172.16.100.93	192.168.151.22(局域网)	HTTP	/py/sql/sqli.php?id=id%3D1+and...
2017-05-08 10:55:53	XPATH注入攻击	172.16.100.93	192.168.151.22(局域网)	HTTP	/py/sql/sqli.php?id=id%3D1+and...

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

The screenshot displays the WAF management console. The left sidebar shows a tree view of site groups under 'root', including 'web\_server', 'test', '123', '实验室环境', 'gg', 'test22', '1234', and '111111'. The main content area is divided into three sections: '站点组基本信息', '站点', and '虚拟站点'. The '站点组基本信息' table lists configurations for the 'web\_server' group. The '站点' table lists individual sites with their types, IP addresses, ports, and certificates. The '虚拟站点' table lists virtual sites with their domains and URI paths.

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	[Icons]

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		🟢	🟢	🟢	[Icons]
12123	HTTPS	1.2.3.4-1.2.3.5	443	2222.cer	🔴	🟢	🟢	[Icons]

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	/*		🔴	🟢	[Icons]
test1	www.test1.com	/*		🔴	🟢	[Icons]

## 策略优化

### 向导模式

创建站点组>向导模式>业务系统信息

#### 操作系统 ^

- 所有类型
- Linux/Unix
- Windows
- Others

#### WEB服务器 ^

- 所有类型
- IIS
- Nginx
- Others
- Apache
- Weblogic
- Tomcat
- Lighttpd

#### 数据库 ^

- 所有类型
- SQL Server
- Postgres
- Others
- Access
- Oracle
- Mysql
- DB2

#### 开发语言 ^

- 所有类型
- PHP
- Java
- Others
- ASP
- Python
- .Net
- Perl

上一步

完成

## 策略优化

### 仅选择准确度高的规则

编辑Web通用防护

动作  ?

源IP封禁

规则信息

匹配原则  匹配中即结束  匹配中仍继续

规则筛选

规则类型 (多选) x 10

ID

危险等级 (多选) x 3

操作系统 (多选) x 3

Web服务器 (多选) x 7

名称

准确度 高

数据库 (多选) x 7

编程语言 (多选) x 7

筛选

规则列表 查看 全部

- 跨站脚本防护
- SQL注入防护
- LDAP注入防护
- SSI指令防护
- XPath注入防护

确定 重置 取消

# 策略优化

## 策略补充

协议校验	
策略模板	
模板快速配置	<a href="#">选择站点模板</a> 应用模板已有配置快速配置下列策略
协议校验	
HTTP协议校验	通用-待优化
基础防护	
HTTP访问控制	通用-待优化
Web服务器/插件防护	紫光阁-待优化
爬虫防护	请选择策略
Web通用防护	紫光阁-待优化
文件非法上传防护	通用-待优化
非法下载限制	通用-待优化
信息泄露防护	通用-待优化
高级防护	
盗链防护	请选择策略
跨站请求伪造防护	请选择策略
扫描防护	通用-待优化
Cookie安全	请选择策略
内容过滤	请选择策略
敏感信息过滤	请选择策略
精准防护	
白名单	请选择策略
其他防护	



## 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

The screenshot shows the '编辑站点' (Edit Site) configuration window in a WAF system. The interface includes a sidebar with site groups, a main configuration area, and a table of supported web servers and languages.

**编辑站点**

服务器名称: qqq \*

服务器类型:  HTTP  HTTPS

服务器IP地址: 1.1.1.1 - 2.2.2.3 \* ?

服务器端口: 443,80 \*

开启Web访问日志:  是  否

开启访问量统计:  是  否

**HTTP解码失败动作:  阻断  放过 ?**

记录内置HTTP协议校验告警日志:  是  否

Web服务器	语言
IIS	PHP
Apache	ASP
Tomcat	.Net
Nginx	Java
Weblogic	Python
Lighttpd	Perl

底部按钮: 确定, 取消

## 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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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.	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

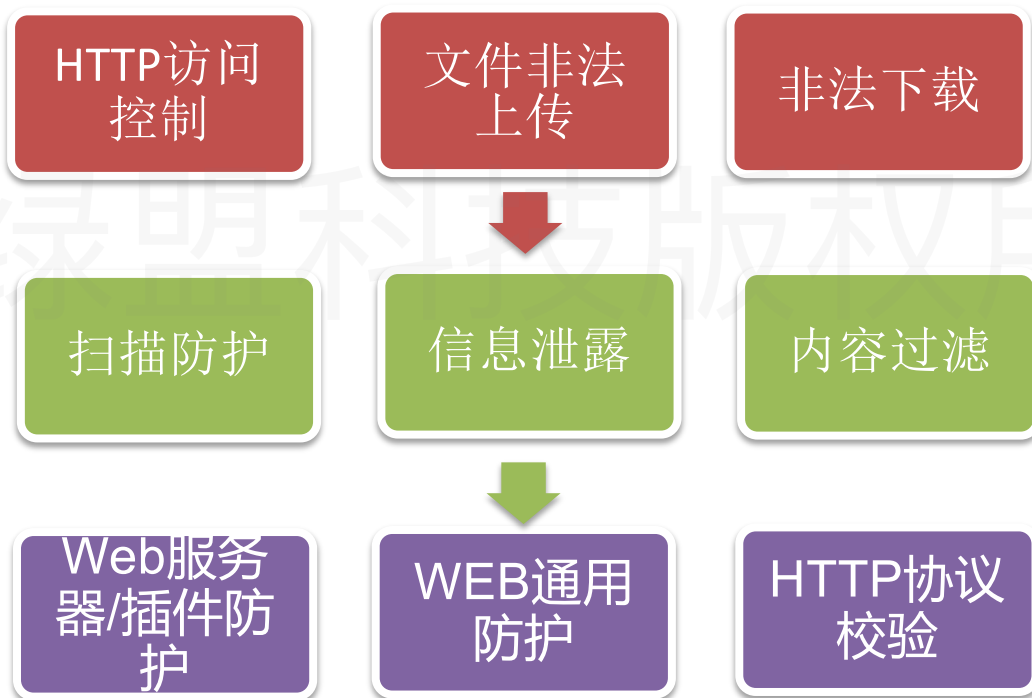
查询所有日志



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	

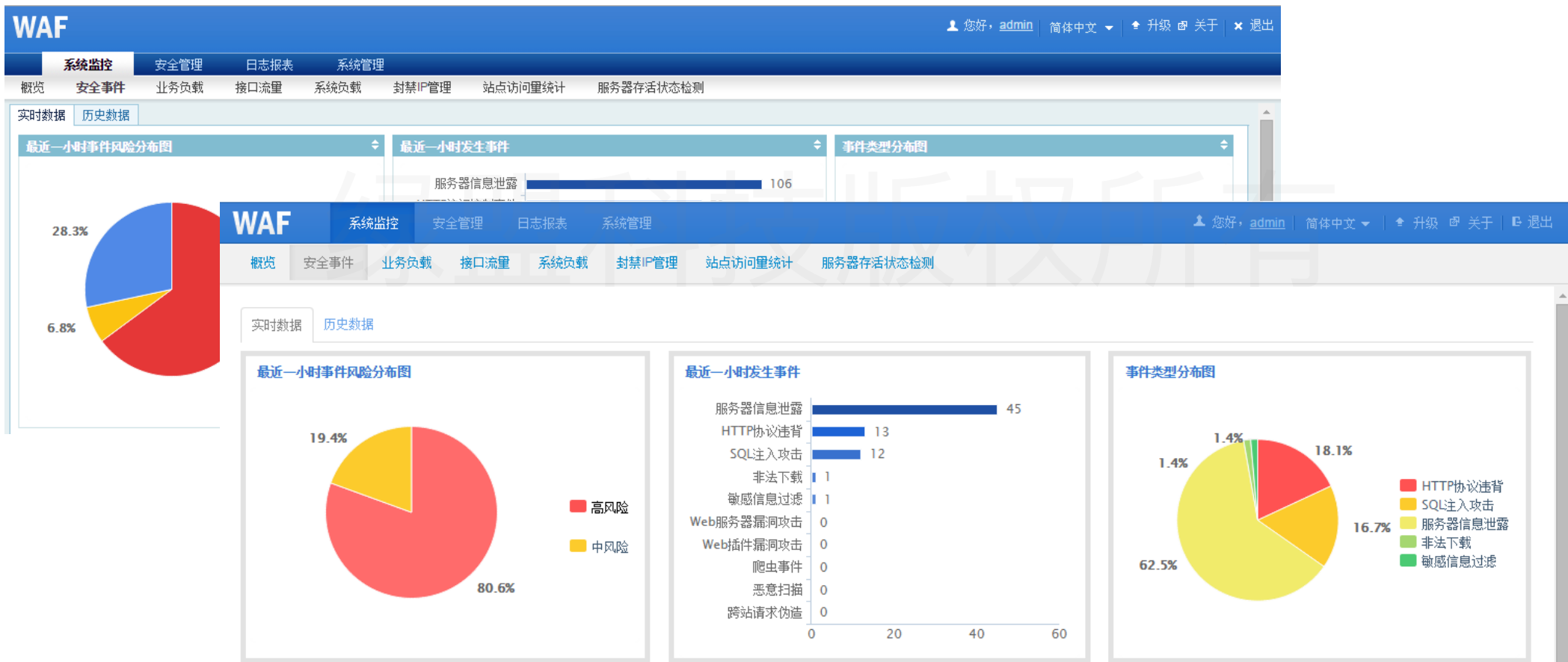
## 策略优化

- 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

绿盟科技版权所有

## ▶▶ 误防处理

绿盟科技版权所有

日志分析



加例外策略  
or调整对应  
防护规则

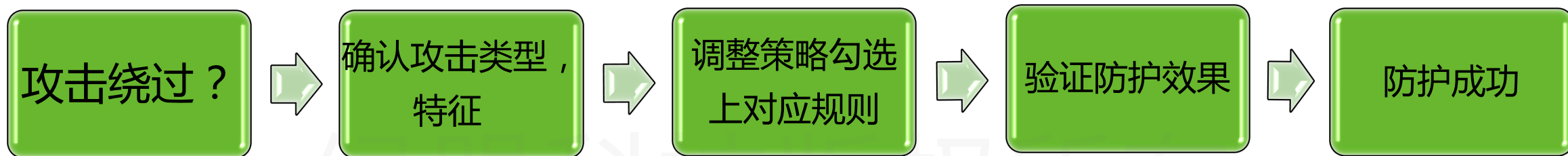


验证问题解  
决





## 漏防处理



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** 系统管理 用户管理 您好, maintainer 简体中文 关于 退出

系统参数配置 系统运维 REST API 站点控制 在线帮助

### 一键收集

一键收集可搜集设备相关信息，便于分析设备异常原因，从而定位故障。

开始收集

文件	大小(MB)	时间	操作
1key_collect_2017_12_26_16_34_22.bin	119	2017-12-26 16:34:35	

### 系统恢复

系统恢复适用于系统进程、数据库、引擎等发生异常时，便于紧急修复。

**数据库**

重建数据库 ?

**进程**

重启WEB服务

重启引擎服务

重启日志服务

**引擎**

生成引擎内存转储 ?

## ▶▶ 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!

绿盟科技版权所有



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

