云枢擎天 WEB 应用防火墙

用户使用手册

版本 V4.0

云枢擎天 WEB 应用防火墙用户使用手册

目录

目录2
第1章 前言 11
1.1 版权声明11
1.2 支持信息11
1.3 手册内容11
1.4 手册约定12
1.5 期望读者13
第2章 帮助系统14
第3章 首页 15
3.1 系统信息16
3.2 系统日志17
3.3 许可状态18
3.4 接口状态18
第4章 系统管理 19
4.1 系统管理介绍19
4.2 系统状态19
4.3 授权信息
4.4 系统升级
4.5 系统诊断
4.6 系统维护24

4.7	7 管理员管理	
	4.7.1 角色管理	25
	4.7.2 用户管理	27
4.8	3 在线用户	29
第5章	配置管理	
5.1	I 配置管理介绍	
5.2	2 网络配置	
	5.2.1 基本网络配置	
	5.2.2 高级网络配置	
	5.2.3 SSH 隧道	
5.3	3 系统配置	
5.4	1 短信发送配置	
5.5	5 邮件发送配置	
5.6	SHA 配置	40
	5.6.1 参数说明	
	5.6.2 部署方法	41
	5.6.3 配置同步	42
	5.6.4 故障与切换	43
	5.6.5 关闭 HA	43
5.7	7 告警配置	44
	5.7.1 Web 攻击告警	44
	5.7.2 网页篡改告警	44

		5.7.3 设备状态告警	45
5	5.8	日志配置	45
		5.8.1 基本配置	46
		5.8.2 日志导出	47
		5.8.3 日志清空	48
		5.8.4 日志服务器	49
5	5.9	配置管理	51
		5.9.1 配置导入	51
		5.9.2 配置导出	52
5	5.10) SNMP 配置	52
		5.10.1 SNMP	52
5	5.11	5.10.2 SNMP Trap	55 .56
第6章	章 5	对象管理	.58
6	5.1	证书管理	.58
		6.1.1 新建证书	.58
		6.1.2 查看详细	.59
		6.1.3 删除证书	.59
6	6.2	会话标识管理	.59
		6.2.1 创建会话标识	.60
		6.2.2 删除会话标识	.60
6	6.3	错误提示页面	.60
		6.3.1 新建错误提示页面	.61

	6.3.2 删除错误提示页面61
6.4	爬虫标识组
	6.4.1 新建爬虫标识组
	6.4.2 编辑爬虫标识组
	6.4.3 查看爬虫标识组
	6.4.4 删除爬虫标识组
	6.4.5 新建爬虫标识
	6.4.6 删除爬虫标识
6.5	扫描器标识组
	6.5.1 新建扫描器标识组
	6.5.2 编辑扫描器标识组
	6.5.3 查看扫描器标识组
	6.5.4 删除扫描器标识组
	6.5.5 新建扫描器标识
	6.5.6 删除扫描器标识
第 7 章	缺省规则67
7.1	规则管理67
第 8 章	策略管理
8.1	策略管理介绍
8.2	策略管理
	8.2.1 添加策略
	8.2.2 删除策略

	8.2.3 编辑策略	.72
8.3	策略模板	.73
8.4	黑白名单	.74
	8.4.1 添加黑白名单	.75
	8.4.2 删除黑白名单	.76
	8.4.3 开启和关闭	.76
8.5	协议规范检测	.77
	8.5.1 配置阈值	.79
	8.5.2 防护动作	.80
	8.5.3 配置例外	.80
	8.5.4 开启和关闭	.81
8.6	输入参数验证	.81
	8.6.1 配置参数验证	.81
	8.6.2 防护动作	.82
	8.6.3 开启和关闭	.83
8.7	访问控制	.83
	8.7.1 配置访问控制	.83
	8.7.2 开启和关闭	.84
8.8	基本攻击防护	.84
	8.8.1 默认规则库	.84
	8.8.2 新建自定义规则	.84
	8.8.3 查看自定义规则	.86

8.8.4 删除自定义规则	86
8.8.5 防护动作	87
8.8.6 应答体检测	87
8.8.7 开启和关闭	87
8.9 盗链防护	88
8.9.1 配置盗链防护8	88
8.9.2 防护动作	89
8.9.3 配置例外	90
8.9.4 开启和关闭	90
8.10 爬虫防护	90
8.10.1 配置爬虫防护	90
8.10.2 防护动作	91
8.10.3 开启和关闭	91
8.11 扫描器防护	91
8.11.1 配置扫描器防护	91
8.11.2 防护动作	92
8.11.3 开启和关闭	92
8.12 暴力浏览攻击防护	92
8.12.1 配置暴力浏览攻击防护	92
8.12.2 防护动作	93
8.12.3 开启和关闭	93
8.13 HTTP CC 防护	93

8.13.1 配置 HTTP CC 防护93
8.13.2 防护动作94
8.13.3 开启和关闭94
8.14 网站隐身
8.15 站点转换
8.16 数据窃取防护
8.17 实时关键字过滤
8.17.1 关键字白名单97
8.18 错误码过滤
8.19 策略生效
8.20 策略浏览
第9章 服务管理 100
9.1 透明模式服务管理100
9.1.1 新建服务100
9.1.2 查看服务101
9.1.3 修改服务101
9.1.4 删除服务102
9.2 反向代理模式服务管理102
9.2.1 新建服务/主机102
9.2.2 查看服务/主机103
9.2.3 修改服务/主机104
9.2.4 删除服务/主机104

9.3 服务状态监控104
第10章 漏洞扫描管理107
10.1 新建漏洞扫描任务107
10.2 查询漏洞扫描任务112
10.3 操作漏洞扫描任务113
第 11 章 网页防篡改118
11.1 防篡改管理118
11.2 防篡改配置119
11.3 镜像同步120
11.4 篡改检测
第12章 日志123
12.1 系统日志
12.2 访问日志124
12.2.1 服务访问日志124
12.3 事件日志125
12.3.1 告警日志125
12.4 防护日志126
12.4.1 防篡改日志126
12.4.2 漏洞扫描日志127
12.4.3 WEB 防护日志128
第 13 章 报表 129
13.1 时段综合统计129

13.2 服务综合统计	
13.3 WEB 攻击统计	
13.3.1 被攻击目标的分布	
13.3.2 按攻击类型统计	
13.3.3 按攻击源地址统计	
13.3.4 按访问方法统计	
13.3.5 受攻击最多的 URLTOP 排名	
附录	
1. 出厂配置	
1.1 通讯口初始配置	
1.2 Web 用户初始配置	
1.3 命令行用户初始配置	
1.4 管理口	
1.5 串口	
2. WAF 在多链路环境下的路由配置	
2.1 WAF 中的路由介绍	
2.2 配置示例	

第1章 **前言**

1.1 版权声明

本手册中的内容是米好信安 WEB 应用防火墙用户使用手册。本材料的相关权力归南 京米好信息安全有限公司所有。使用手册中的任何部分未经本公司许可,不得转印、影印 或复印。

由于产品版本升级或其它原因本使用手册内容会不定期进行更新,除非另有约定本使 用手册仅作为使用指导,本手册中的所有陈述信息和建议不构成任何明示或暗示的担保。 本声明仅为文档信息的使用而发表,非为广告或产品背书目的。

1.2 支持信息

本资料将定期更新,如欲获取最新相关信息,请查阅公司网站:https://www.mhxa. net.cn/

1.3 手册内容

首先感谢您使用米好信安的网络安全产品。本手册为 WEB 应用防火墙(以下简称为 "WAF")用户使用手册,对其使用与配置做了详细的介绍。本手册的内容包括以下各章:

- 第1章:前言。包含版权声明、支持信息、手册内容、手册约定以及期望读者等
 内容。
- 第2章:帮助系统。描述 WAF 产品的帮助系统的使用方法。
- 第3章:首页。描述 WAF 产品首页中包含的内容,主要包括网站防火墙数据统
 计、系统信息、系统日志、WEB 服务器运行状态、许可状态、接口状态等。

- 第4章:系统管理。描述 WAF 的系统管理,主要包括系统状态、授权信息、系统升级、规则库升级、系统诊断、系统维护、管理员管理、在线管理员等。
- 第5章:配置管理。描述 WAF 的基本配置信息,包括网络配置、系统配置、短信发送配置、邮件发送配置、HA 配置、告警配置、日志配置、配置管理、报表配置、SNMP 配置、管理配置等。
- 第6章:缺省规则。介绍 WAF 的 web 攻击防护的缺省策略配置功能。
- 第7章:策略管理。介绍 WAF 的 web 攻击防护的策略配置功能。
- 第8章:服务管理。介绍WAF的不同工作模式下的服务的新建、修改和删除以及服务状态监控等。
- 第9章:对象管理。介绍证书、会话标识、爬虫标识组、扫描器标识组和错误提示页面的新建、删除等功能。
- 第10章:漏洞扫描管理。介绍WAF的漏洞扫描功能,包括漏洞扫描任务的新建、编辑、执行、删除以及报告的查看等。
- 第 11 章:网页防篡改。介绍 WAF 的网页防篡改功能。
- 第 12 章: 日志。介绍 WAF 的日志功能。
- 第13章:报表。介绍WAF的各类报表功能。
- 第14章:附录。介绍WAF一些补充说明信息,包括WAF系列产品的出厂默认
 配置、多链路环境下的路由配置和独立日志管理系统。

1.4 手册约定

为方便用户阅读与理解,本手册遵循以下约定:

〕
一
使用技巧、建议和引用信息等



⚠______重要信息

【XXX】——菜单名称和按钮名称的表示方式

注1:本文中所有图例均为屏幕截取。

注 2:本文中 Web 界面部分所有图片均为通过 IE 访问的界面。

注 3: Web 界面中所有需要输入的 IP, 其格式均为: 点分十进制形式 (*.*.*.*)。

1.5 期望读者

期望了解本产品主要技术特性和使用方法的用户、系统管理员、网络管理员等。本文 假设您对下面的知识有一定的了解:

- 系统管理
- Linux 和 Windows 操作系统
- Internet 协议
- 网络安全

第2章 **帮助系统**

用户登录后,可看到右上角的欢迎信息,如图所示。这里可以进行用户个人信息编辑,查 看到用户所属角色,查看帮助信息,和注销当前用户。



图 2-1 系统欢迎条

"帮助"功能是当用户定位到某一系统模块时,提供相应的该模块的帮助信息。例如,首 页帮助信息,是在首页时点击帮助弹出的帮助信息页面。帮助页的开始是模块基本介绍和内容 导航,后面是详细功能介绍。如下图:

首页
系统首页 系统首页列出系统中查看蛇频繁或观注度较高的部分信息,通过系统首页可对系统的运行及状态有初步了解。系统首页目 前包括如下内容:
 网站防火螺数螺统计 系統信息 系統日志 WEB服务器运行状态 许可状态 接口状态
网站防火墙数据统计
网站防火炮数据统计主要为系统WEB攻击防护部分的攻击事件统计,统计内容包括:
 美型 - WEB攻击关型 总计 - 显示每种攻击进型的总数 今天 - 显示每天的攻击统计数量,统计时间段为00:00:00到当前的时间 本小时 - 显示最近一小时统计数量
系统信息
系统信息列出系统当前的状态信息,具体显示内容包括:
 设备型号 - 当前设备的产品型号 设备应列号 - 显示此设备被授权的序列号 主机名称 - 素统名称 软件板本号 - 显示当的系统使用的软件板本 系统助问 - 当前系统的时间 最近升级时间 - 系统当前CPU使用信况,百分比显示 CPU利用率 - 系统当前内存使用信况,百分比显示 内存利率 - 系统当前内存使用信况,百分比显示 主/备角色 - 显示双机始督状态 部署模式 - 显示双前始督状态 - 置示系统当前BYPASS状态,直通时系统将不进行数据处理。
系统日志

图 2-2 首页帮助信息

第3章 **首页**

首页是合法用户登录后首次看到的页面,其主要内容有网站防火墙数据统计、系统信息、 系统日志、WEB 服务器运行状态、许可状态、接口状态等几个部分。系统每隔 15 秒自动刷新 首页信息。用户可以手动隐藏、刷新或关闭某个部分。

系统信息		2 \$ X	系统日志					@ 1K
信息	状态		用户	1	寧件	摘要	状态	
设备数号	DCFW-1800-WAF2046		admin	1	制式服务的连闭性	服委名称:test	1 失敗	
设备序则号	20130304waf05069994300501011		admin		改業 22	新建防着改服务	: 咸功	
主机名称	DOWWAF		admin		0DosR8#	認知(COoS語語)日	14 成功	
软件版本号	4.0.1.11		capyt		服务管理	新建服务,名称:	大 成功	
系统时间	2013-03-12 10:50:12 (21)		xiecm	1	用户放弃	xiezm用户等录系	1 15.13	
运行时间	0天 0小村 30分		capyi		服务管理	偏振服装,名称	+ 10.03	
量近升切时间	##d		admin		服务管理	新建田道, 名称	+ #13	
CPU利用率	F 2%		admin		8422	BREE, CR	+ #135	
內存利用率	27%		- decar		84.90	1000 E.H. (100		
HA当前状态	来启动		olares .		8.70-E	NORTH COL	+ efth	
容器模式	乐路模式		aomin	- 1	5754 5768	MIRS / 58.	- et 19	
bypass铁态	車直遷訳志(两道)		admin	- 1	0.9 B 12	新建築会・名称、	7, MLAO	
许可状态		A 0 X	接口状态				1	# X
(6.0.	状态		(2.0	eth0	eth1	eth2 et	ha	ethe
许可贷款	正式原		状态			A		100
硬件ID	E896-27CD-2EAF-9878							Panel 1
系统有效期限	N/A		12.4	1000ME	ars 1000Mb/s	*		1

图 3-1 WAF 首页





系统日志	5				× ¢ ×
接口状系	5			(* # X
信息	eth0	eth1	eth2	eth3	eth4
状态					
速率	1000Mb/s	1000Mb/s	-	-	-
模式	Full	Full	24	23	125
接收	1.2 GiB	180.0 b	0.0 b	0.0 b	0.0 ł
发送	154.1 KiB	78.3 MiB	0.0 b	0.0 b	0.0 ł
<)			>

图 3-3 隐藏一个窗口

执行隐藏或是关闭了窗口后,再次点击左侧导航链接"首页",系统会重新装载、显示全部的窗口。

3.1 系统信息

系统信息显示 WAF 设备的基本信息,如设备型号、设备序列号、主机名称、软件版本号、 系统时间(可以通过【编辑】快速进入到配置中的"时间配置页面")、运行时间、最近升级时 间、CPU 利用率、内存利用率和部署模式(透明模式、反向代理模式)、bypass 状态等信息。 如下图所示:

系统信息	
信息	状态
设备型号	waf-546
设备序列号	mhhwaf20150209000001
主机名称	WAF (<u>编辑</u>)
软件版本号	4.0.1-20141213
系统时间	2014-12-23 10:41:09 (編輯)
运行时间	1天 1小时 2分
最近升级时间	2014-12-18 08:55:50
CPU利用率	0%
内存利用率	0%
HA当前状态	未启动
部署模式	透明模式
bypass状态	非直通状态(waf-546)

图 3-4 系统信息

点击"主机名称"或"系统时间"中的蓝色【编辑】链接,可对相关信息进行编辑,如下



图:

主机名称配置		
	主机名称: WAF	字母开头,字母、数字、下划线和中划线组成,长度为1到20
		确定 取消



	系统时间:	2013-03-12 10:57:11			
 手动i 	25番时间:	2013-03-12 10:57:09		C	与本地时间同步
〇 时间	服务器:	1.pool.ntp.org	如:1.pool.ntp.org	, time	.windows.com@



3.2 系统日志

系统日志记录了用户最近对 WAF 进行操作所生成的系统日志,记录了系统日志的用户、 事件、摘要和状态,如下图所示:

系统日志			\$\$X
用户	亊件	摘要	状态
lifang	协议规范	配置协议规范	成功
lifang	协议规范	配置协议规范	成功
lifang	协议规范	配置协议规范	成功
lifang	协议规范…	配置协议规范	成功
lifang	基本攻击…	配置基本攻击	成功
lifang	暴力浏览…	配置暴力浏览…	成功
lifang	暴力浏览…	配置暴力浏览	成功
lifang	服务管理	编辑服务ws_1…	成功
lifang	暴力浏览	配置暴力浏览	成功
lifang	暴力浏览	配置暴力浏览	成功
shenxma	告警配置	DDoS攻击告	成功

图 3-7 系统日志

3.3 许可状态

许可状态显示 WAF 系统中 License 的授权情况,包含许可类型、硬件 ID、系统有效期限、 规则库有效期限等。如下图所示,系统有效期限为 "N/A"代表这是个正式版的 License,不 会过期;规则库有效期限将于 730 天后过期。

许可状态		\$\$X
信息	状态	
许可类型	正式版	
硬件ID	9673-5B2E-7691-6739	
系统有效期限	N/A	
规则库有效期限	2014-07-05 (剩余730 天)	

图 3-8 许可状态

3.4 接口状态

接口状态显示了 WAF 设备上各个接口的状态,包括速率、模式、接受和发送的流量等信

息。如下图所示:

接口状态				*	x
信息	eth0	eth1	eth2	eth3	e
状态					
速率	1000Mb/s	1000Mb/s	1000Mb/s	1000Mb/s	-
模式	Full	Full	Full	Full	-
接收	844.1 MiB	410.2 MiB	70.7 KiB	3.0 MiB	0
发送	63.6 MiB	221.0 MiB	284.8 KiB	538.3 KiB	0
<	1111				>

图 3-9 接口状态

第4章 **系统管理**

4.1 系统管理介绍

WAF 的系统管理主要包括以下各项:

- 系统状态
- 授权信息
- 系统升级
- 系统诊断
- 系统维护
- 管理员管理
- 在线用户

<u>
八
注意事项:</u>

为不同的对象命名时,系统不支持以下特殊符号:逗号(,)、单引号(")以及双引号("")。 为避免产生错误,建议用户尽量使用数字(0-9)和字母(a-z, A-Z)组成对象名称。对 象名称的长度限制在1到20个字符。

4.2 系统状态

系统状态下,可查看系统的"接口流量统计"、"CPU利用率"、"内存利用率"等状态。

接口流量统计是设备各个接口接收和发送的流量统计,如图所示。默认显示的为接收流量统计,点击"发送流量"则显示发送流量统计。不同接口的流量用不同的颜色标识,通过勾选/取消勾选来显示/不显示该接口的流量(默认为显示所有接口的流量)。将鼠标停留在统计图的



某一时刻,则会有文字显示该接口的实时流量。



图 4-1 接口流量统计





图 4-2 CPU 利用率





图 4-3 内存利用率

查看系统状态有两种方式:(1)自定义时间段查询,(2)快捷查询。

快捷查询,系统预置了五种方式:最近1小时、昨天、今天、最近7天、最近30天。

如果快捷查询的时间段不能满足用户需求, WAF 还提供了自定义显示时间的方法。用户可

自定义起始时间和结束时间,然后点击【查看】按钮即可。

点击页面右上角的它可以将当前页面导出为 html 页面。

4.3 授权信息

授权信息页面用于显示当前 license 信息以及升级 license 文件。

license 文件包含授权用户、授权状态、保护服务数、系统版本、授权模块等信息,用户可在本页面查看 license 信息,如下图所示。

授权信息		
授权信息		
	授权用户:	
	授权状态:	正式版
	保护服务数:	10(个)
	系统版本:	4.0
	授权植块:	[WEB防护][DDoS攻击防护][漏洞扫描][防麴改][站点加速][关键字防护][HA(双机热备)][网站分析]
	硬件ID:	470F-B102-E741-FAC0
	产品序列号:	
	规则库有效期:	剩余 309 天
导入授权		
	授权证书:	选择文件 未选择任何文件 导入 注: 授权证书文件必需为(.crt)格式,大小不超过10K
	硬件特征码:	470F-B102-E741-FAC0

图 4-4 授权信息

用户单击【浏览】按钮,从本地选择授权文件,然后单击【导入】,会显示证书信息,如下 图所示,确保证书无误后,点击【确定】,即可导入成功。重新打开授权信息页面,即可查看授 权文件信息。

₩ 八双枚 证书信息:	授权信息: 授权用户: 授权状态:正式版 保护服务数:5 授权模块: [WEB助护] [贏洞扫描] [防篡改] 硬件释征值: 57A6-804A-C08A-3A6D 产品序列号: 20120410waf0506999290005101100000730
	确定 取消

图 4-5 授权信息 2

⚠_{注意事项:}

请联系厂商的销售人员,获得 WAF 的授权文件,并确定与所购买产品硬件的型号匹配。

如果用户购买的授权文件中,没有许可某个模块的使用,那么该模块将不可配置。

为了避免许可证使用期限缩短,请在导入许可证之前,确保正确的系统时间。

4.4 系统升级

系统升级用于系统版本更新和版本信息的显示,系统升级有手动升级和自动升级两种方式。

界面如下图所示。

杀统并级			
版本信息			
	软件版本:	4.0.1-20141213	
	规则版本:	10.0.1-20141213	
手动升级			
	升级包:	选择文件 未选择任何文件	升级 注:升级包文件必需为(.tar.bz2)棺式,大小不超过50M

图 4-6 系统升级界面

- 1) 版本信息:版本信息显示当前版本号和规则版本号。
- 2) 手动升级:当用户的升级包保存在本地时,使用该方式。用户点击【选择文件】从本 地选择一个升级包,再点击【升级】即可实现升级。

<u>
八
注意事项:</u>

手动升级时,请联系厂商的技术支持人员,获得升级包,并确定是否与产品硬件的型号匹 配。

为避免并发升级对系统产生异常,自动升级开启后不能执行手动升级。

升级过程比较长,请耐心等待升级成功。

4.5 系统诊断

提供用户对系统配置的诊断和查看功能,包含 ping 工具诊断、系统自检和网络信息查看。 1)工具诊断:用户提供可视化 ping 命令工具,输入主机 IP、发包数和网口,点击执行即

可。如下图所示。



图 4-7 系统诊断

2) 系统自检:点击【开始系统自检】按钮,系统开始网络配置等信息进行自检,并输出,

如下图:



图 4-8 系统自检



3) 网络信息查看:用户可以 ARP 表、路由表、策略路由、网卡等信息,点击相应按钮即

可,如下图所示。

网络信息查看	
查看ARP表 查看主路由表 查看管理口策略路由 查看网卡信息	
Kernel IP routing table	A
Destination Gateway Genmask Flags Metric Ref Use Iface	
152.152.152.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1	
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 0 管理口	
182 182 0 0 0 0 0 255 255 0 U 0 0 0 eth0	
192158450 0000 2552550 1 0 0 0 0 4 4 1	
109.254.0.0 0.0.0.0 255.255.0.0 0 0 0 0 管理目	
0.0.0.0 182.182.182.254 0.0.0.0 UG 0 0 0 eth0	~
	×

图 4-9 网络信息查看

4.6 系统维护

为用户提供直通切换、关机、重启和恢复出厂设置等功能,如下图所示。

系统维护		
0	非直通状态 可以切换为直通状态	切换为:直通状态
0	系统关机 将当前设备关闭	关机
0	系统重启 将当前设备重新启动	重日
Ø	恢复出厂设置 将当前设备恢复出厂设置	恢复出厂设置



⚠_{注意事项:}

WAF 运行在反向代理模式时,不支持直通切换功能。



4.7 管理员管理

管理员管理用于超级管理员进行管理系统权限分配的角色和基于角色的用户,以达到对指定的用户授予恰当的角色权限来执行系统操作。界面如图所示。

		用户自	1年 用巴目	旺	
系统		用白鹭	今1田		
系统状态		лал-те	54E		
授权信息		1	新建		
系统升级		序号	用户名	角色名称	电子邮箱
规则库升级		1	admin	超级管理员	
病毒库升级		2	test	系统管理员	
系统诊断					
系统维护	=	-			
管理员管理					
在线用户	1				
配置					

图 4-11 管理员管理界面

管理员管理包括角色管理和用户管理两部分。角色管理是用户权限分配的基础,通过角色 管理可以将系统指定模块的查看或执行权限进行分配。用户管理是管理可以登录系统的用户信 息,其权限主要基于所属的角色。

⚠_{注意事项:}

只有超级管理员才有管理员管理权限。

4.7.1 角色管理

选择角色管理标签进行角色的配置,系统内置的角色包括:

WAF 内置的的角色包括四类: 系统管理员 (除管理员管理外的所有系统权限), 审计管理员 (对系统状态、日志、报表进行审计和导出权限), 配置管理员 (对系统的配置权限), 更新管理员 (对网站防篡改的操作权限)。系统内置角色权限不能修改。通过"查看权限"或操作列

下的 🤤 按钮可以查看角色的权限, 通过"查看用户"可以查看属于该角色的用户列表。管理

界面如图所示。

角色管	理			每页显示 20 ▼ 約	┣, 当前第1/1页 │ \
7 Я	新建				
序号	角色名称	来源	权限	属于该角色的用户	操作
1	系统管理员	系统内置	查看权限	查看用户	¢)
2	审计管理员	系统内置	查看权限	查看用户	4
3	配置管理员	系统内置	查看权限	查看用户	4
4	更新管理员	系统内置	查看权限	查看用户	4
5	只读	用户自定义	查看权限	查看用户	4 🗗 🛍
6	执行	用户自定义	查看权限	查看用户	(1) 10 10 10 10 10 10 10 10 10 10 10 10 10

图 4-12 角色列表

4.7.1.1 新建角色

管理员也可以通过建立自定义角色对特定的模块进行授权。通过"新建"创建自定义角色,

如图,选择相应的只读和执行权限给角色,确定后新建成功。

新建角色				
*角色名:				
权限分配		只读 🔲	执行 🔳	
□系统				
·	系统状态			
	授权信息			
	系统升级			
	规则库升级			
[病毒库升级			
[系统诊断			
	系统维护			
	在线用户			
三 配置				
	网络配罟			

图 4-7 新建角色



若赋予某一模块执行权限,则自动选中该模块的只读权限,因为执行权限级别更高。

4.7.1.2 编辑角色

点击需要修改的自定义角色条目中的 建按钮,可以编辑该角色的权限。"角色名"不能更改。

4.7.1.3 删除角色

点击要删除的自定义角色条目中的 🏛 按钮, 可以删除该角色。

<u>
八
注意事项:</u>

已经被用户在使用的角色,不能直接删除,应当先删除相应用户再删除角色。

4.7.2 用户管理

选择用户管理标签进行系统用户的管理。admin 超级管理员是系统内置的用户,具有管理系统的一切权限。

用户管理	里 角色管理				
用户管	理			每页显示 20 ▼条,当前	前第1/1页 🛛 🖓 [<mark>1</mark>
1	师建				
序号	用户名	角色名称	电子邮箱	登录IP	操作
1	admin	超级管理员			🛃 🗑
2	test	系统管理员			📝 🛍

图 4-14 用户管理

4.7.2.1 新建用户

点击页面的 → 新建按钮,新建一个用户。用户名、角色、密码为必填项,电子邮箱、授 权登录 IP 为选填项。

"角色名称"项是下拉选项,可以为用户选择系统内置角色或自定义角色,选择后可通过 右侧的"查看权限"按钮查看所选角色具有的权限。"授权登录 IP"是指允许使用该新建用户 登录使用的 IP,多个 IP (最多 10 个 IP)之间用半角的逗号分隔,如果留空表示不受限制。

建用户	
*用户名:	
*角色名称:	系统管理员 💙 查看权限
*密码:	
*确认密码:	
电子邮箱:	
	<u>^</u>
授权登录IP:	
	~

图 4-8 新建用户

4.7.2.2 编辑用户

点击用户列表中需要编辑用户条目的 [▶]按钮,可以编辑该用户的信息。"用户名"不能更改,"密码"和"确认密码"在编辑时显示为空,如果不需要修改密码则不要编辑。 <u>▲</u>注意事项:

该模块功能仅适用于 admin 用户进行管理员管理,每个用户若要编辑自己的信息需要点 击右上角欢迎条的 // 且用户名和所属角色不能自己修改。

4.7.2.3 删除用户

点击要删除的用户条目中的 🏛 按钮, 可以删除该用户。

<u>
八
注意事项:</u>

系统默认 admin 用户不能被删除。



4.8 在线用户

在线用户用于查看当前使用系统的用户信息,界面如图所示。

在线用	户			每页显示 20 ▼条,当	前第1/1页 🛛 🖓 [1] 🕅
序号	用户名	角色名称	登陆时间	源IP	查看日志
1		系统管理员	2013-03-18 16:45:02	192.168.2.113	查看日志
2		系统管理员	2013-03-18 16:07:54	172.16.21.116	查看日志

图 4-9 在线用户界面

在线用户信息包括:用户名、角色名称--用户所属角色名称,登录时间--用户登录进入系统的时间,源IP—用户登录系统所用的IP,查看日志—查看用户操作系统日志。

选择在线用户"查看日志",以查看该用户执行了哪些系统操作。如图所示,可以查看某一 在线用户的系统日志列表。查看完后点击"返回"可以返回到原来的"在线用户"界面。

查看系	(绂日志caoyj <u>返回</u>	1				
14	Page 1 of 4	> > @			Dis	playing 1 - 40 of 136
	时间	登录IP	事件	摘要	日志级别	状态
1	2013-03-18 16:45:02	192.168.2.113	用户登录	caoyi用户登录系统	信息	成功 🔶
2	2013-03-18 16:45:02	192.168.2.113	用户管理	caoyj用户,源地址为: 172	信息	成功
3	2013-03-18 16:44:45	192.168.2.113	用户登录	caoyi用户登录系统	错误	失败
4	2013-03-18 16:43:29	172.16.21.115	用户登录	caoyi用户登录系统	信息	成功
5	2013-03-18 16:42:33	172.16.21.115	用户登录	caoyi用户注销登录	信息	成功
6	2013-03-18 16:12:38	172.16.21.115	配置管理	导出成功	信息	成功
7	2013-03-18 16:12:10	172.16.21.115	用户登录	caoyi用户登录系统	信息	成功
8	2013-03-18 16:12:09	172.16.21.115	用户管理	caoyi用户,源地址为: 192	信息	成功

图 4-10 查看在线用户操作日志

<u> 八 注意事项:</u>

查看在线用户权限只有特定角色的用户才可以使用,系统内置角色中,超级管理员和系统 管理员具有该权限,审计管理员、配置管理员和更新管理员都不能查看在线用户。

第5章 配置管理

5.1 配置管理介绍

WAF 的配置管理主要包括以下各项:

- 网络配置
- 系统配置
- 短信发送配置
- 邮件发送配置
- HA 配置
- 告警配置
- 日志配置
- 配置管理
- SNMP 配置

5.2 网络配置

配置的部署方式,以及在不同部署方式下的各个网口的 IP 地址、子网掩码、静态路由和策略路由,实现 WAF 在网络中的正确部署和运行。

该模块还包含 SSH 隧道配置,以便在特殊情况下进行远程协助环境的搭建。

<u>
八 注意事项:</u>

网络配置设置的正确与否影响到设备能否正常工作,用户要小心设置。

5.2.1 基本网络配置

基本网络配置根据应用环境的不同分为透明模式、和反向代理模式,通过点击不同的单选

按钮进行切换,如下图所示:

基本网络配置 运行模式			
	模式选择:	◉ 透明模式	◎ 反向代理模式
		保存	

图 5-1 运行模式选择

<u>
八
注意事项:</u>

在透明模式下可以进行桥 IP、管理口以及 DNS 的配置;在反向代理模式下可以进行 WAN

口、LAN 口、管理口以及 DNS 的配置。具体如下:

1) 桥 IP 配置,设置桥 IP 地址、子网掩码和默认网关,然后【保存】,即可完成配置,如

下图所示:

桥IP配置 [br_default(eth0,eth1)]	
IP地址:	182.182.182.141
子阿掩码:	255.255.255.0
默认网关:	182.182.254
	保存

图 5-2 桥模式下桥 IP 配置

在反向代理模式下可配置 WAN 口、LAN 口 IP 地址以及掩码。

2) WAN 口配置, 设置 IP 地址、子网掩码和默认网关, 在透明模式下, 不可配置, 如下

图所示:

WAN口配置 [eth0]		
IP地址:	182.182.182.141	
子网掩码:	255.255.255.0	
默认网关:	182.182.182.254	
	保存	

图 5-3 反向代理模式下 WAN 口配置

2) LAN 口配置,在透明模式下,不可配置,如下图;



LAN口配置 [eth1]	
IP地址:	0.0.0
子网掩码:	0.0.0
	保存

图 5-4 反向代理模式下 LAN 口配置

3) 管理口配置,设置 IP 地址、子网掩码即可完成修改,系统默认无地址,如下图:

管理口配置 [eth5]		
IP地址:	172.16.21.141	
子网掩码:	255.255.255.0	
	保存	

图 5-5 管理口配置

4) DNS 设置,设置系统使用的首选 DNS 服务器地址和备选 DNS 服务器地址,如下图所

示。

DNS设置	
首选DNS服务器:	8.8.8.8
备选DNS服务器:	
	保存



↓ 如果 DNS 为空, 或 DNS 不能正常使用, 请在新建保护服务时, 正确填入保护服务所 有的 IP 地址。

5.2.2 高级网络配置

根据产品运行的模式的不同,可以设置的内容不尽相同。在透明模式下,可以进行网桥配置、VLAN 配置、静态路由配置和策略路由配置;在反向代理模式下,可以进行 WAN 口虚拟 IP 配置以及静态路由和策略路由配置。

5.2.2.1 网桥配置

在网桥配置部分可以查看当前网桥列表、也可以对已建网桥进行编辑,或者删除网桥。

网桥列表页面显示网桥名称、网口列表、IP 地址、掩码等信息,如下图:

阿桥配置				
🌛 新建				
网桥	网口列表	IP地址	掩码	操作
br_default	eth0,eth1	182.182.182.141	255.255.255.0	3
br_qiao1	eth6,eth7	172.16.25.23	255.255.255.0	🛃 🖬



5.2.2.1.1 新建网桥





新建网桥时需要输入网桥名称,选择需要的网口。

<u>
八 注意事项:</u>

每个网桥至少由2个网口组成。

eth0和eth1默认属于br_default网桥,不可从br_default桥中删除,但可以向br_default 桥中增加网口。

5.2.2.1.2 编辑网桥

以系统管理员角色登录后,点击网桥列表页中相应条目的【 📝 】 图标,即可进入编辑网



图 5-9 编辑网桥界面

<u>
八 注意事项:</u>

每个网桥至少由2个网口组成。

eth0和eth1默认属于br_default网桥,不可从br_default桥中删除,但可以向br_default 桥中增加网口。

5.2.2.1.3 删除网桥

点击网桥列表页中某条记录中的【 1 发钮, 在出现的确认窗口选择【 确定】, 即可删除 该网桥。

<u>
八
注意事项:</u>

绑定服务的网桥或者有 VLAN 关联的网桥不能被删除。

5.2.2.2 VLAN 配置

在 VLAN 配置部分可以查看当前 VLAN 列表、也可以对已建 VLAN 进行编辑,或者删除



VLAN.

VLAN 列表页面显示 VLAN 名称、ID、网口、IP 地址、掩码等信息,如下图:

VLAN配置					
🥪 新建					
VLAN	VLAN ID	MD	IP	掩码	操作
v_100	100	br_default	122.23.23.23	255.255.255.0	🖻 🖬
v_200	200	br_default	0.0.0	0.0.0.0	🚽 🛍

图 5-10VLAN 列表

5.2.2.2.1 新建 VLAN

点击 VLAN 列表界面的【 📝 新建… 】按钮,进入新建网桥界面。如下图所示。

新建VLAN	
VLAN名称:	
VLAN ID:	(2~4094)
网口:	br_default 💌
	确定 取消

图 5-11 新建 VLAN 界面

新建 VLAN 时需要输入名称, VLANID、网口等信息。

5.2.2.2.2 编辑 VLAN

以系统管理员角色登录后,点击 VLAN 列表页中相应条目的【 📝 】图标,即可进入编辑

VLAN 界面进行编辑,如下图所示:

编辑VLAN		
VLAN名称:	v_100	
VLAN ID:	100 (2~4094)	
四口:	br_default	
IP地址:	122.23.23.23	
子网掩码:	255.255.255.0	
	确定取消	

图 5-12 编辑 VLAN 界面

5.2.2.2.3 删除 VLAN

点击 VLAN 列表页中某条记录中的【 ¹¹ 】按钮,在出现的确认窗口选择【确定】,即可删 除该 VLAN。

<u>
八 注意事项:</u>

绑定服务的 VLAN 不能被删除。

5.2.2.3 静态路由配置

在页面中输入网络地址、子网掩码、网关,网口可以新建一条静态路由,也可以通过点击 每条路由后面的删除按钮删除该条路由。如下图:



图 5-13 静态路由配置界面

5.2.2.4 策略路由配置

在页面中输入网络地址、子网掩码、网关,网口可以新建一条静态路由,也可以通过点击

每条路由后面的删除按钮删除该条路由。如下图:

策略路由配置				
网络地址	子网掩码	网关	网口	操作
0.0.0.0	0.0.0.0	0.0.0	管理口 💙	0
0.0.0.0	0.0.0.0	172.16.21.254	管理口	Ť

图 5-14 策略路由配置界面


5.2.2.5 WAN 口虚拟 IP 配置

在页面中输入 IP 地址、子网掩码、网口可以为 WAN 口新建一个虚拟 IP, 也可以通过点

击每条虚拟 IP 后面的删除按钮删除该条路由。如下图:

WAN口度換IP配置				
IP地址	子网掩码	网口	操作	
		WAN	0	
192.168.53.23	255.255.255.0	WAN	Ť	

图 5-15WAN 口虚拟 IP 配置界面

5.2.3 SSH 隧道

SSH 隧道分为配置和开启/关闭操作两部分。

1) SSH 隧道配置, 输入公共服务器的 IP 地址以及建立隧道的端口即可, 其输入范围, 在

页面上有提示,如下图:

SSH隧道配置	
IP地址:	124.16.26.25
端口号:	7001
	保存

图 5-16SSH 隧道配置

2) 隧道的启停: SSH 隧道配置后,可以通过按钮进行启动和关闭,如下图所示:

SSH隧道操作		
隧道操作:	开启隧道 关闭隧道	

图 5-17SSH 隧道操作

5.3 系统配置

可以配置系统的时间或者与 NTP 服务进行时间按同步, 也可以修改 WAF 设备的名称。如



下图:

时间服务器配置		
系统时间	2013-03-27 15:36:53	
◎ 手动设置时间:	2013-03-27 15:35:07	与本地时间同步
○ 时间服务器:	1.pool.ntp.org	如:1.pool.ntp.org、time.windows.com等
		确定取消

图 5-18 时间配置

用户可以手动修改当前时间,也可以设置时间服务器,当时间服务器可用时,系统会自动 同步时间。

同时,用户可以在该页面进行主机名称配置,如下图:

主机名称配置	
	主机名称: WAF 字母开头,字母、数字、下划线和中划线组成,长度为1到20
	确定 取消

图 5-19 主机名称配置

5.4 短信发送配置

通过配置短信发送设备,系统可以提供短信告警功能,可以检测短信发送设备是否正常:

如下图,

短信管理
短信设备测试
点击开始测试: 短信设备测试

图 5-20 短信设备检测

若短信发送设备在线,可以通过输入合适的手机号码进行测试,如下图:



发送测试短信			
岩信接 (☆문码:	भूमित रेजी	

图 5-21 短信设置测试页面

5.5 邮件发送配置

通过设置发件人邮件地址、SMTP的服务器信息以及登录信息,可实现邮件服务器的配置,

如下图,

邮件发送配置	
发信人信息	
邮箱地址:	gengtao20022002@126.com
服务器信息	
发送邮件服务器(SMTP):	smtp.126.com
服务器端口(默认值25):	25
登录信息	
登录用户名:	gengtao20022002
登录密码:	•••••
	保存重置

图 5-22 邮件服务器配置

- > 发信人信息:填写一个邮箱,需要发送邮件时就用这个邮箱发送。
- 服务器信息:填写一个邮件服务器和服务器端口,端口时默认的 25,邮件服务器根据所用邮箱的不同而不同,比如 126 邮箱的邮件服务器是 smtp.126.com, 163 邮箱的邮件服务器是 smtp.163.com。
- > 登录信息:填写发件箱的用户名和密码。一定要填写正确,否则不会成功发送邮件。

用户配置完成并保存后,可以通过输入自己的邮件地址进行测试(需要 WAF 设备能连通 外网),如下图:



邮件测试

测试邮箱地址:

■ **发送测试邮件** 邮件服务器配置完成后,建议您发送测试邮件,以确保配置成功。(需要网络支持)

图 5-23 邮件设置测试页面

若成功,则给用户以成功提示,自己的收件箱中也会受到测试邮件。

5.6 HA 配置

高可靠性 (High Availability),简称为 HA,能够在通信线路或设备产生故障时提供备用 方案,从而保证数据通信的畅通,有效增强网络的可靠性。实现 HA 功能,用户需要配置两台 采用完全相同硬件平台、固件版本的 WAF。当一台设备不可用或者不能处理来自客户端的请 求时,该请求会及时转到另外的可用设备来处理,这样就保证了网络通信的不间断进行,极大 地提高了通信的可靠性。

本章按照透明模式和反向代理模式分别讲解 HA 的部署。

5.6.1 参数说明

配置界面如下图所示:

HA配置			
▲工作状态-			
	运行模式: 透明代理模式		
	HA 处于不工作状态		
	*HA服务:	◎开启 ◉关闭	
	*设备角色:	◉主机 ○从机	HA启动流程是先配置主机,然后再配置从机,请勿颠倒次序
	*心跳间隔:	1秒 ▼	
	*心跳口:	eth2 🔻	
	*本端地址:	3.3.3.1	
	*对端地址:	3.3.3.2	
			确定重置
	同步配置: 执行	当前状态为激活时才可以进行同步操作	

图 5-24 透明模式 HA 配置



各参数配置说明如下:

- > 设备角色: 主机、从机; 请按照先主机后从机的顺序配置
- 心跳口:主从设备心跳链路的物理接口,可以选择除管理口以外的所有物理网口。主 从设备的心跳链路必须是一条通路,以保证主从设备通信的心跳包可以正确送达。心 跳包采用组播方式由激活设备从心跳口发送,主从设备的心跳口 IP 必须不一致,才 能正常收发,如果选择了当前系统中没有 IP 的物理接口,需配置该接口的 IP 地址。 主从设备的心跳口可以直连,也可以通过交换机等设备链接,只要保持通路即可。主 从设备的心跳口须一致。

日 若心跳口为直连,监控链路中请勿勾选心跳口。

- 心跳间隔:激活设备向未激活设备发送心跳包的时间间隔,间隔越短,识别故障并执行业务切换的时间越短。同时,如果时间间隔过短,故障识别敏感度越高,一两个丢包也可能导致切换,请根据自身网络质量合理选择,推荐值3秒。主从设备的心跳间隔须一致。
- 对端地址:主从设备进行配置同步时,需要知道对端的 IP 地址,填写为对端设备的 心跳口 IP。
- > 本端地址: 本端的 IP 地址,填写为本端设备的心跳口 IP

5.6.2 部署方法

1. 配置前检查:



- ▶ 确认两台 WAF 设备硬件型号一致,软件版本一致,且具有 HA 功能。
- > 完成网络配置,包括创建网桥,配置接口 IP 地址等
 - 本 HA 只支持网桥模式下运行;
- > 被监控的链路已经插好网线且连通 (否则启动 HA 后会监控链路异常)。
- 2. 进行主设备配置,参数说明参见 5.6.1 或 5.6.2:
- 3. 进行从设备配置,参数说明参见 5.6.1 或 5.6.2

主从设备需要配置相同的心跳口,心跳间隔,,对端地址填写互相的 HA 口(心跳口)地 址。

4. 确认主从设备心跳线已经连接好,

心跳接口可以是直连或者通过交换机连接到系统上。如果 HA 接口是直连, 请不要选择 HA 口为监控链路。

5. 确认主从 HA 参数配置好后就可以启动 HA 服务了

5.6.3 配置同步

HA 环境部署完成后, 配置 WAF 时, 只需在激活设备上进行配置, 新加入的配置可以通过 自动同步和手动同步两种方式同步至未激活设备。

配置同步依赖于三个条件:

1.主从设备的对端地址配置正确

2.网络通畅

3.主从设备的系统版本一致。

配置手动同步:

当管理员修改激活设备的配置信息后,点击 HA 配置页面-同步配置-执行,可以手动将配

置同步至未激活设备。该功能一般无需使用,仅作为检验配置是否能正确同步的一种手段。

1 配置同步不包含网络配置信息。

5.6.4 故障与切换

WAF 设备 HA 模块故障监控的范围为:

- > 工作机 (激活状态) 出现宕机 (重启);
- > 工作机 (激活状态) 掉电;
- > 监控链路网口故障 (网口链路不通,网线未插好)。

当出现上述情形之一时, 激活设备进入故障状态, 未激活设备进入激活状态, 开始接管业

务。故障设备从故障中恢复后,进入未激活状态(若为主机优先为是的主机,则抢占当前业务,

进入激活状态)。

UHA 对系统的软件状态不做监控。

5.6.5 关闭 HA

成功部署 HA 后,如需关闭 HA,请按照一下步骤操作:

1.未激活设备上,拔掉所有网桥内网口网线 (反向代理模式下无需拔线),关闭 HA。

2.激活设备上,关闭 HA。

↓ 若需要从反向代理模式下关闭 HA,请在关闭 HA 之前删除所有服务。

如果已经关闭了 HA, 还需要删除服务, 请执行以下操作:

1.保留管理口网线,其他全部移除。

2.重新开启 HA, 配置为主机, 监控链路一个都不选, 开启后, 即可删除服务

3.删除服务后,关闭 HA。

5.7 告警配置

告警是指当受保护服务受到攻击时、设备状态达到警戒线或者被保护的主机出现异常时, 采取某种方式向管理人员报告,目前支持邮件告警和短信告警两种模式。

5.7.1 Web 攻击告警

默认显示的告警类型是"Web 攻击告警",如下图所示,通过该界面,可以进行的设置有:

- ▶ 告警开关:开启或关闭 web 攻击告警;
- > 发送间隔:设置多长时间发送一次告警;
- 告警方式:有邮件和短信告警两种方式;
- > 接收邮箱/接收手机号码:填写一个可用的邮箱和手机号码,每个文本框最多填写10

个。

告響管理-WEB 攻击告響			
告警开关:	🖲 开启 🔍 关闭		
发送间隔:	5	分钟	
告鑿方式:	✔邮件 □短信		
接收邮箱:	meng1103@126.com		邮件之间用半角的速号(即英文的逗号)分隔; 仅允许输入10个Email。
是否发送摘要信息:	◎否 ●是		
		保存重置	

图 5-25Web 攻击告警设置界面

5.7.2 网页篡改告警

网页篡改告警列表页面如下图所示。



告警管理-阿页篡改告警					
序号	服务名称	告警状态	邮件	短信	操作
1	test	开启	gengtao20022002@126	15801313449	2

图 5-26 网页篡改告警列表

点击操作栏的"修改"链接进入设置网页篡改告警页面,如下图。篡改告警在每个检测任

务执行完毕发现有篡改行为后进行,其参数设置参考"Web 攻击告警"节。

告警管理-编辑网页篡改告警			
服务名称:	test		
告警开关:	⊙ 开启 ○ 关闭		
发送间隔:	5 分钟		
告警方式:	☑ 邮件 ☑ 短信		
接收邮箱:	gengtao20022002@126.com .::		邮件之间用半角的逗号(即英文的逗号)分隔; 仅允许输入10个Email。
接收手机号码:	15801313449		手机号码之间用半角的逗号(即英文的逗号)分隔; 仅允许输入10个手机号码。
		确定取消	

图 5-27 网页篡改告警设置界面

5.7.3 设备状态告警

设备状态告警设置如下图所示,参数设置参考"Web 攻击告警"节。

告警管理-设备状态告警		
日志空间检测:	◉是 ◎否	
设备占用空间:	80	% 请在日志高:置模块中编辑,超过此值则告警
内存检测:	● 是 ◎ 否	
内存占用空间:	88	% 大小请输入 1 到 95(%),超过此值则告警
告警开关:	🖲 开启 🔍 关闭	
发送间隔:	5	分钟
告警方式:	■邮件 □短信	
擦收曲降:	meng1103@126.com	邮件之间用半角的逗号(即英文的逗号)分隔; 仅允许输入10个Email。
		保友 垂雲

图 5-29 设备状态告警设置界面

5.8 日志配置

日志配置包括基本配置、日志导出、日志清空、日志服务器四个部分,这四部分通过选项 卡进行选择。



点击左侧导航"配置"-"日志配置"项,进入日志配置的主界面,如下图所示。

• 首页	基本配置 日志异出 日志語空 日志屬冬粟
 系统 	
- 配質	基本配置
网络配置	▲ 存錄空间
时间配置	使用字: 0%
短信发送配置	
邮件发送配置	
HA配置	
告警配置	· 确定 重畳
日志配置	



5.8.1 基本配置

基本配置页面可以查看当前存储空间的使用情况,如下图:

存储空间	
使用率:	■ 15% 总大小:94.1MB 空闲大小:80.1MB

图 5-29 存储空间使用情况

日志记录方式包括磁盘记录、内存记录和不记录三种方式,通过选择单选按钮来实现不同

的选择。如下图。

基本配置 日志导出 日志清	空 日志服务器			
基本配置				
▲ 存储空间				
使用率:		1% 总大小: 917GB 空闲大小: 869GB		
·····································				
◎ 磁盘记录	◎ 不记录			
*最大占用率:	80	大小请输入 1 到 95(%)		
*超过上限时:	不记录] 当存储超过所设置的占用率时,执行的操作		
	日志类型	保存天数	是否记录	
系统日志	系统日志	* 41		
访问日志	服务访问日志	* 36	×	
事件曰志	告警日志	* 3	8	
	WEB防护日志	* 3	×	
防护日志	防篡改日志	* 2	9	
	漏洞扫描日志	* 15	9	
		石前元	ē 重置	

图 5-30 日志基本配置

最大占用率指的是,日志大小占总空间大小的比率。

基本配置部分对各个字段的解释如下:

- ▶ 磁盘记录:将生成的日志记录到硬盘。
- ▶ 不记录:不记录日志。
- 超过上限时:用户可以设置当存储空间(硬盘、内存)达到一个值时,对日志的处理, 处理的动作是"不记录"两种。比如,可以设置当内存占用达到90%时,重写最早日志。
- ▶ 日志类型:描述了九种日志类型。
- 保存天数: 默认为 15 天, 超过 15 天的日志将自动被删除。用户可以根据需要配置 为需要保存日志的时间范围。
- > 是否记录:可以对六种日志进行是否记录的选择。

<u>
八 注意事项:</u>

WAF 每分钟检测日志大小是否超过了设置的设备占用率,如果超过了,WAF 将删除最早 一天生成的日志,直至低于设置的设备占用率。

5.8.2 日志导出

日志手动导出。手动导出为手动下载方式。通过选中对应的单选按钮,进行方式的选择,

如下图所示。

基本教授 日志等出 日志講会 日志服务器	
日志写出	
选择导出方式	
	● 手动导出

图 5-31 日志导出方式

当选择手动导出时,页面显示如下图:



释导出方式				@ x5-4E40
				· 于约马卫
用时间集和日志类型				
开始时间: 2014-12-23 🔤	结束时间	: 2014-12-23		
	□全法	日志类型	大小	
系统日志		系统日志	96K	
访问日志		服务访问日志	16K	
事件日志		击撃日志	280K	
		WEBBPHE	20K	
攻击日志		防整改日志	12K	
		精制描目志	36K	

图 5-38 日志导出-手动导出

用户可以选择生成日志的时间和类型进行导出。导出后解压数据包,双击文件"系统日志



******.cvs" 文件查看, 如右图所示。

手动下载就是将一定时间内的日志导出到本地

5.8.3 日志清空

通过选择被清空的日志类型,可以单选或者"全选",点击【清空】按钮,即可清除对应的日志记录,如下图所示。

清空 选择日志类型				
开始时间: 2017-01-09		结束时间: 2017-01-	09	
	□全选	日志类型	大小	
系统日志		系统日志	72K	
访问日志		服务访问日志	28K	
事件曰志		告警日志	288K	
		WEB防护日志	24K	
防护日志		防篡改日志	412K	
		漏洞扫描日志	144K	
				清空重置

图 5-39 日志清空



5.8.4 日志服务器

日志服务器功能是指 WAF 可以配置日志服务器的信息,通过 syslog 协议,经由网络导出系统中指定的日志。配置 syslog 日志服务器,方便用户对多日志服务器集中且安全地管理。

日志服务器显示页面如下图所示:

日志服	5番						
》 添	加						
序号	名称	服务器IP	端口	状态	协议类型	日志类型	操作
1	test	1.2.3.4	514	0	udp	服务访问,WEB防护,服务监控	\$\$\$ \$\$\$\$ \$

图 5-32 日志服务器

新建成功的日志服务器在页面上显示的信息有:序号、名称、服务器 IP、端口、状态、协议类型、日志类型和操作。

5.8.4.1 新建日志服务器

点击"添加"按钮,新建日志服务器页面如下图:

日志服务器		
*名称:		字母开头,字母、数字和下划线组成,长度为1到20
*服务器IP:		
*诗耑口:		(1~65535)
协议类型:	UDP V	
*日志类型:	□ 服务访问日志 □ WEB防护日志 □ 服务监控日志	本功能将导出所连日志到syslog日志服务器
		确定即消

图 5-33 新建日志服务器

对各个字段的解释如下:

- > 名称:日志服务器的名称,两个日志服务器的名字不能相同。
- ▶ 服务器 IP: syslog 日志服务器的 IP。
- ▶ 端口: syslog 日志服务器的端口。
- > 协议类型:有 UDP 和 TCP 两种类型。协议类型和端口一定要与日志服务器上的协议

U

类型和端口一致。

日志类型:可以选择导出到日志服务器的日志类型,可以单选或者多选。包括服务访问日志、web访问日志、服务监控日志三种类型。

5.8.4.2 操作日志服务器

可以对建立好的日志服务器进行关闭/开启、编辑、删除等操作。当关闭日志服务器时,日 志将不能导出到日志服务器。

> 关闭日志服务器

选择一个日志服务器记录, 点击"操作"列的"关闭"按钮, 将对此日志服务器执行关闭。

如下图所示。

基本配置	日志导出 日志	宇空 日志服务器					
日志服务	꿇						
🥜 添	10						
序号	名称	服务器IP	端口	状态	协议类型	日志类型	操作
1	ww	192.168.2.19	514	0	udp	服务访问,WEB防护,服务监控	(🖓 🕞 👘

图 5-42 日志服务器关闭

▶ 编辑日志服务器

选择一个"关闭"状态的日志服务器,点击"操作"列的"编辑"按钮,将对此日志服务器执行编辑。当此日志服务器的状态是"运行"时,不能进行编辑,系统将弹出提示信息"请先关闭日志日志服务器,再执行编辑",如下图所示。



关闭日志服务器后,如下图所示



日志服务	2						
🌛 添加							
序号	名称	服务器IP	端口	状态	协议类型	日志类型	操作
1	ww	192.168.2.19	514	•	udp	服务访问,WEB防护,服务监控	🎯 🛃 🛍

图 5-43 日志服务器编辑

▶ 删除日志服务器

选择一个日志服务器记录,点击"操作"列的"删除"按钮,将对日志服务器记录被删除。

5.9 配置管理

配置管理功能主要用来实现配置的转移,便于用户维护和管理系统配置。

5.9.1 配置导入

配置管理页面如下图所示

配置管理		
配置导入		
	配置文件:	选择文件 未选择任何文件 國置号入 注: 電型文件必需为(.do) 裕式, 大小不趨过2004, 请先上传配置文件, 再进行导入操作
配置导出		
		配适号出

图 5-34 配置管理

用户可以点击"浏览"按钮,从本地保存的配置文件中选择要导入的配置文件,然后点

击"配置导入"按钮,检查无误后,可以点击【确定】按钮,就会导入这个配置文件了。

<u>
八
注意事项:</u>

导入配置的时候,系统会重启,重启之后新的配置才会生效。



5.9.2 配置导出

配置导出可以将 WAF 当前的配置导出到本地,以备以后用时方便直接导入。

点击配置管理页面的【配置导出】按钮, 就可以将 WAF 当前配置导出到本地。

配置管理	
配置导入	
配置文件:	送 禄交仲 未选择任何文件 截置与入 注: 配置文件必需为(.dg/k式,大小不超过20M,请先上传配置文件,再进行导入操作
配置导出	
	配法导出

5.10 SNMP 配置

本功能用于对 WAF 设备的 SNMP 和 SNMP trap 服务进行配置。

5.10.1 SNMP

SNMP 根据版本的不同,其配置参数不同,分别说明如下:

5.10.1.1 SNMP V1 和 V2C

配置界面如下:

NMP配置			
SNMP代理:	◎ 开启 ○ 关闭		
SNMP版本:	⊙V1 ○V2c ○V3		
读写权限:	只读权限 🗸		
SNMP团体:	public	以字母开头,字母、数字和下划线组成,长度为1	到20
IP: 子网掩码:		ada	
	192.168.0.0/255.255.0.0	NCN.	
官理碼IP网段列表:		除选中	

图 5-47 SNMP v1 和 v2c 配置页面



其参数说明如下:

- > SNMP 代理:开启或关闭 SNMP 代理服务,关闭 SNMP 代理后,仍可以更改 SNMP 的 配置。
- 读写权限:下拉列表中包括"只读权限"和"读写权限"。配置"只读权限"时,SNMP管理端可以获取WAF的信息,但不能更改WAF的信息。配置"读写权限时",SNMP管理端可以获取或修改WAF的信息。默认为"只读权限",若无通过SNMP管理端修改WAF信息的需求,建议选择"只读权限"。
- SNMP 团体:用于验证管理端是否有权限访问 WAF,仅当 SNMP 管理端配置的 SNMP 团体名称与该处配置的名称一致时,才可获取 WAF 设备信息。SNMP 团体名称以字母开 头,字母、数字和下划线组成,长度为 1 到 20。默认值为 public,建议配置时修改 SNMP 团体名称。

5.10.1.2 SNMP V1 和 V2C

配置界面如下:

SNMP配置		
SNMP代理:	◎开启 ○关闭	
SNMP版本:	Ov1 Ov2c ⊙v3	
用户级别:	○无认证无加密 ○认证无加密 ④认证加密	
读写权限:	只读权限 🖌	
用户名:	lyt_1234567	以字母开头,字母、数字和下划线组成,长度为1到20
认证方式:	●MD5 ○SHA	
人证密钥:	******	以字母开头,字母、数字和下划线组成,长度为8到20
确认认证密钥:	******	
加密方式:	● DES ○ AES	
加密密钥:	******	以字母开头,字母、数字和下划线组成,长度为8到20
确认加密密钥:	••••••	
言任的管理端网段		
IP:		
子网摘码:	添加	

图 5-48 SNMP v3 配置页面

其参数说明如下:

- > SNMP 代理:开启或关闭 SNMP 代理服务,关闭 SNMP 代理后,仍可以更改 SNMP 的 配置。
- 用户级别:用于配置验证 SNMP 管理端访问权限的安全级别,包括无认证无加密、认证无加密、认证无加密、认证加密三种级别。默认为认证无加密级别。
- 读写权限:下拉列表中包括"只读权限"和"读写权限"。配置"只读权限"时,SNMP管理端可以获取WAF的信息,但不能更改WAF的信息。配置"读写权限时",SNMP管理端可以获取或修改WAF的信息。默认为"只读权限",若无通过SNMP管理端修改WAF信息的需求,建议选择"只读权限"。
- 用户名: SNMP V3 版本用于验证管理端来源的用户名称,以字母开头,字母、数字和下 划线组成,长度为1到20。
- 认证方式:认证密钥的加密方式,当用户级别为认证无加密和认证加密时,可配置。有 MD5、 SHA 两个可选项,默认为 MD5 方式。
- 认证密钥:当用户级别为认证无加密和认证加密时,可配置。以字母开头,字母、数字和 下划线组成,长度为8到20。
- 加密方式:加密密钥的加密方式,只有当用户级别为认证加密时,可配置。有 DES、AES 两个选项,默认为 DES 方式。
- 加密密钥:只有当用户级别为认证加密时,可配置。以字母开头,字母、数字和下划线组成,长度为8到20。

5.10.1.3 信任的管理端网段

仅当管理端 IP 属于管理端 IP 网段列表中的某个信任网段时,才允许其通过 SNMP 管理

WAF 设备。

在IP输入文本框中填写信任的管理端IP网段,在子网掩码输入框中填写相应的子网掩码。 点击"添加"按钮,再点击"确定",则填写的管理端IP网段和子网掩码就会进入到管理端IP 网段列表中。也可以多次添加网段/子网掩码,再点击"确定",将多个网段加入管理端IP网段 列表。

若要从管理端 IP 网段列表中删除某个或多个网段,则在管理端 IP 网段列表中选中所有要删除的网段/子网掩码,点击"删除选中",再点击"确定"即可。

<u>
八
注意事项:</u>

SNMP代理占用WAF的端口为161。

5.10.2 SNMP Trap

SNMP Trap 配置页面如下图:

SNMP Trap	
SNMP Trap配置	
是否发送Trap:	③是 ○否
接收的管理端IP和端口	
接收Trap的管理端IP:	
接收Trap的管理端端口:	162 添加
管理端IP和端口列表:	192.168.2.194:165 金田 御殿途中
Trap项配置	
Trap项配置:	 ☑ CPU利用率超过80% ☑ 磁磁利用率超过80% ☑ 最近一分钟攻击備況 ☑ 図内口连接 ☑ 図内口断开
	· 本宁 王忠

图 5-49 SNMP Trap 配置页面

参数说明如下:

▶ 是否发送 Trap:是否向 SNMP 管理端发送 Trap 信息,有"是"、"否"两个选项,默认为

"否"。

- ➢ 接收的管理端 IP 和端口:当发送 Trap 消息时,仅向管理端 IP 和端口列表中的 I 地址发送 Trap 消息。
 - 接收 Trap 的管理端 IP: 指定管理端 IP
 - 接收 Trap 的管理端端端口:配置指定的端口 (默认 162)
 - 添加:点击该按钮,可将配置的 IP 和 port 对添加进列表中
 - 若要从管理端 IP 和端口列表中删除某个或多个 IP:端口,则在管理端 IP 和端口列表 中选中所有要删除的 IP:端口,点击"删除选中",再点击"确定"即可。
- > Trap 项配置: 该项配置用于选择向管理端发送 Trap 信息的类型, 默认为全选。
 - CPU 利用率超过 80%: 当 CPU 利用率大于或等于 80%时触发该 Trap 信息。
 - 磁盘利用率超过 80%: 当磁盘利用率大于或等于 80%时触发该 Trap 信息。
 - 内存利用率超过 80%:当内存利用率大于等于 80%时触发该 Trap 信息。
 - 系统重启: 若系统重启, 会在系统启动后触发该 Trap 信息。
 - 网口连接: 当网口连接时触发 Trap 信息。
 - 网口断开:当网口断开时触发 Trap 信息。

5.11 管理配置

管理配置的主要功能是配置访问 WAF 管理界面的协议类型 (HTTP 或 HTTPS) 和端口。 界面如下:

管理配置		
允许HTTP访问:	● 是 ○ 否	默认:禁用HTTP访问Web管理界面
HTTP端口:	80	默认:80
允许HTTPS访问:	●是 ○否	默认:只允许HTTPS访问Web管理界面
HTTPS端口:	443	默认:443
		确定 重置

图 5-50 管理配置界面

- ▶ 允许 HTTP 访问 配置是否允许以 HTTP 协议访问 Web 管理界面,默认为不允许。
- ▶ HTTP 端口 如果选择允许 HTTP 访问,则需要配置 HTTP 端口,默认为 80。
- ▶ 允许 HTTPS 访问 配置是否允许以 HTTPS 协议访问 Web 管理界面,默认为允许。
- ▶ HTTPS 端口 如果选择允许 HTTP 访问,则需要配置 HTTPS 端口,默认为 443。

本功能允许同时配置两种协议类型和相应的端口访问 WAF 管理界面。提交配置之前,会 检测配置的端口,在当前系统运行过程中是否被其他程序占用,如果被占用,将不允许配置, 可改用其它端口配置。

第6章 对象管理

6.1 证书管理

证书用于网关和客户端或者后台站点之间的认证使用。有两种证书,分别为网关证书和 CA 证书;本模块提供了这两种证书的新建、详细信息查看和删除功能。

证书种类:

CA 证书:在 WAF 中,主要用于识别用户身份,验证客户端提交的客户端证书。

网关证书:服务器证书和客户端证书的合称。WAF 在网络中充当代理,向客户端提交的是服务器证书,向网站服务器提交的是客户端证书,所以当代理前后均需 https 通信的情况下,要求同时提供服务器证书和客户端证书。

证书查看列表如下:

证书管理					
→ 新建					
序号 证书名称 证书类别 默认证书 终止日期	操作				
1 DefaultGateWayCert 网关证书 是 2021-12-31 23:06:16	4				
删除命行选					

图 6-1 证书管理界面

6.1.1 新建证书

通过输入证书名称、选择证书类别、证书格式以及通过浏览选择合适的证书文件,即可进 行证书的导入,如下图:

新建证书			
证书名称:	字母开头,字母、数字和下划线组成,长度为1到20		
证书类别:	 ○ CA证书 ◎ 网关证书 		
证书:	30 览 注: 阿关证书中需包含私钥信息		
证书格式:	● pem格式 〇 pfx格式		
	确定 取消		

6-2 新建证书界面

WAF 支持两种证书格式 pem、pfx, pem 格式为 openssl 所采用的证书格式, pfx 是微软所采用的证书格式。

6.1.2 查看详细

选择证书列表中"操作"列中的"详细"链接即可实现证书详细信息的查看,如下图:

详细信息				
序列号:	08ED151A4BFE72BD4E66C30DEE373553			
证书名称:	CA			
证书类别:	CA证书			
默认证书:	否			
主题:	CN=WAF			
颁发者:	CN=WAF			
有效起始日期:	2011-05-19 13:29:01			
有效终止日期:	2021-05-19 13:38:17			
	确定			

图 6-3 证书详细信息

6.1.3 删除证书

选择证书列表中"操作"列中的"¹¹"链接即可实现证书的删除。

6.2 会话标识管理

浏览器的会话使用存储在 SessionID 属性中的唯一标识符进行标识。会话 ID 使 ASP.NET 应用程序能够将特定的浏览器与 Web 服务器上相关的会话数据和信息相关联。会话 ID 的值 在浏览器和 Web 服务器间通过 cookie 进行传输,如果指定了无 cookie 会话,则通过 URL 进行传输。本模块可以创建会话标识在策略的 HTTPCC 防护、会话跟踪模块中应用。

6.2.1 创建会话标识

创建会话标识包括填写会话标识符名称、会话参数类型、匹配模式、会话参数名称、参数 值起始分隔符、会话参数值、参数值终止分隔符,其中,会话参数类型只能选择 COOKIE。如 下图所示:

会话标识符名称	会话参数类型	匹配模式	会话参数名称	参数值起始分割符	会话参数值	参数值终止分割符	选项
	COOKIE	正则匹配 💟		-		;	添加
php	COOKIE	正则匹配	phpsessid	=	\w{32}	;	ũ
asp2	COOKIE	正则匹配	passwd	-	\w{16}	;	ũ
asp	COOKIE	正则匹配	aspsession	=	[a-z]{24}	;	ũ
MuiX2132au	COOKIE	正则匹配	MuiX_\d{4}	=	[\w/\+]+	;	ũ
MuiX2132au	COOKIE	正则匹配	MuiX_2132	=	.*	;	Ű

图 6-4 会话标识管理

6.2.2 删除会话标识

选择证书列表中"选项"列中的""" 链接即可实现会话标识的删除。

6.3 错误提示页面

点击导航菜单中的【对象库】-【错误提示页面】即可进入错误提示页面列表界面。该模块

显示预定义的错误提示页面列表,如下图所示:

云枢擎天 WEB 应用防火墙用户使用手册

序号	错误提示页面名称	描述	选项
1	default	default page	Q)
2	e400		۵ 🛱
3	e401		۵ 🛱
4	e402		۵ 🛱
5	e403		۵ 🛱
6	e404		۵ 🛱
7	e405		۵ 🛱
8	e406		۵ 🛱
9	e407		۵ 🛱

图 6-5 错误提示页面列表

点击列表中"选项"中的【^{QQ}】可以查看错误提示页面的详细内容,以浏览器的方式打开 该错误提示页面。

6.3.1 新建错误提示页面

新建错误提示页面,需要填写错误提示页面名称,然后选择浏览选择作为错误提示页面的

html 或者 htm 文件,可以对该页面添加描述以方便区分。如下图所示:

新建错误提示页面	
错误提示页面名称:	只允许字母和数字,a-z,A-Z,0-9,最大长度20字符
选择页面:	浏览 只支持html、htm两种棺式,大小限制为100K
描述:	● 最大长度50字符
	确定 重置

图 6-6 新建错误提示页面

6.3.2 删除错误提示页面

支持对自定义错误提示页面的删除操作,单击每条错误提示页面操作栏的【 2011 】 按钮,删除该行的错误提示页面。

6.4 爬虫标识组

爬虫标识指互联网中爬虫的特征,网络爬虫一般在 User-Agent 报头中标识自己的身份。

爬虫标识组作为爬虫标识的集合,与策略-爬虫防护关联,作为爬虫防护的对象。默认组 DefaultRobots 中内置了 161 个恶意爬虫特征。

本模块提供新建、删除自定义爬虫标识,新建、编辑、删除爬虫标识组功能。

6.4.1 新建爬虫标识组

填写爬虫标识组名称,点击添加按钮。新添加的爬虫组,将包括当前所有爬虫标识作为组成员。如下图所示。

爬虫标识组 爬虫标识					
爬虫标识组					
爬虫标识组名	3称: group2	添加 字母开头,字母、数字和下划线线	且成,长度为1到20		
序号	选择	爬虫标识组名称	操作		
1		DefaultRobots	4		
2		group1	(1) 10 10 10 10 10 10 10 10 10 10 10 10 10		
全选 🔽 删除所选					

图 6-7 新建爬虫标识组

五想要新建的爬虫组生效,需在策略-爬虫防护中与其关联,详见相关章节。

6.4.2 编辑爬虫标识组

点击爬虫组右侧编辑按钮,进入爬虫标识组编辑页面。如下图所示。勾选的爬虫标识为当前爬虫组中的成员;如需排除某爬虫,将勾选取消后,点击确定即可。编辑已经在使用中的爬虫组后,会立刻生效。

同时编辑过程中,可以使用搜索功能快速定位某个爬虫。

↓ 为避免爬虫组为空,用户至少要保留一个爬虫在组中。

爬虫标识组 爬虫标识

编辑爬虫标识组【gr	oup1]		
请选择搜索条件	▼ 等于	▲ 査询	
序号		爬虫标识特征	类型
1		webmole	默认 🔶
2		wisenutbot	默认
3		prowebwalker	默认
4		hanzoweb	默认
5		email	默认
6	V	gameBoy, powered by nintendo	默认
7		missigua	默认
8		poe-component-client	默认
9		emailsiphon	默认
10		adsarobot	默认
11	V	under the rainbow 2.	默认
12		nessus	默认
13	V	floodgate	默认
14		email extractor	默认
15		webaltbot	默认
	-		
		确定 取消	

图 6-8 编辑爬虫标识组

6.4.3 查看爬虫标识组

点击爬虫组右侧【 🍳 】按钮,可快速查看该爬虫组中的成员。

6.4.4 删除爬虫标识组

单击爬虫组右侧【 1 发钮,即可删除无用的爬虫组。

□ 已经与策略中爬虫防护关联的爬虫组,需要先取消关联再删除。

6.4.5 新建爬虫标识

选择爬虫标识选项卡,填入爬虫标识,点击添加按钮即可。如下图所示。



云枢擎天 WEB 应用防火墙用户使用手册

爬虫标识组 爬虫标识

爬虫标识			每页显示 20 💌 条,当前第	第9/9页 ¥
爬虫标识特征:		添加		
请选择搜索条件	▶ 等于	▲		
序号	选择	爬虫标识特征	类型	操作
161		mozilla/2.0 (compatible; newt activex; win32)	默认	
162		spider1	自定义	Ű
全诜 🗌 翩綜師诜				

图 6-9 新建爬虫标识

记若想要新建的爬虫标识生效,需要将其加入到爬虫组中。见 6.4.3

6.4.6 删除爬虫标识

点击爬虫标识右侧【 1 发钮,即可删除无用的爬虫标识。

只能删除自定义爬虫标识,如需删除多个,请勾选多个后,点击删除所选按钮。

6.5 扫描器标识组

扫描器标识指网站安全检测工具的特征,这些扫描器一般在 User-Agent、其他报头、URL 中含有独特的标识。扫描器标识组的组织形式与爬虫标识组类似。

扫描器标识组作为扫描器标识的集合,与策略-扫描防护关联,作为扫描防护的对象。默认组 DefaultScanners 中内置了 21 个扫描器标识。

本模块提供新建、删除扫描器标识,新建、编辑、删除扫描器标识组功能。

6.5.1 新建扫描器标识组

填写扫描器标识组名称,点击添加按钮。新添加的扫描器标识组,将包括当前所有扫描器标识作为组成员。如下图所示。



扫描器标识组 扫描器标识

扫描器标识组								
扫描器标识组名称: group2 添加 字母开头,字母、数字和下划线组成,长度为1到20								
序号	选择	扫描器标识组名称	操作					
1		DefaultScanners	4					
2		group1	🏟 🛃 🖆					
全选 🔲 删除所选								

图 6-10 新建扫描器标识组

记 若想要新建的扫描器标识组生效,需在策略-扫描防护中与其关联,详见相关章节。

6.5.2 编辑扫描器标识组

点击扫描器标识组右侧编辑按钮,进入扫描器标识组编辑页面。如下图所示。勾选的扫描器标识为当前扫描器标识组中的成员;如需排除某扫描器标识,将勾选取消后,点击确定即可。 编辑已经在使用中的扫描器标识组后,会立刻生效。

同时编辑过程中,可以使用搜索功能快速定位某个扫描器标识。

▶ 为避免扫描器标识组为空,用户至少要保留一个扫描器标识在组中。

编辑扫描者	器标识组 【grou	p1]		
请选择搜	索条件	(等于	查询	
序号		扫描器标识特征	匹酉社或	类型
1	V	metis	User-Agent	默认 🔺
2	\checkmark	bilbo	User-Agent	默认
3		n-stealth	User-Agent	默认
4		black widow	User-Agent	默认
5	V	brutus	User-Agent	默认
6		cgichk	User-Agent	默认
7	~	webtrends security analyzer	User-Agent	默认
8		mozilla/4.0 (compatible)	User-Agent	默认
9	\checkmark	jaascois	User-Agent	默认
10		pmafind	User-Agent	默认
11		.nasl	User-Agent	默认
12		nsauditor	User-Agent	默认
13		paros	User-Agent	默认
14		nessus	User-Agent	默认
15	V	nikto	User-Agent	默认
			确定 取消	

图 6-11 编辑扫描器标识组

6.5.3 查看扫描器标识组

点击扫描器标识组右侧【 🔍 】按钮,可快速查看该扫描器标识组中的成员。

6.5.4 删除扫描器标识组

单击扫描器标识组右侧【 1 发钮,即可删除无用的扫描器标识组。

U 已经与策略中扫描器防护关联的扫描器标识组,需要先取消关联再删除。

6.5.5 新建扫描器标识

选择扫描器标识选项卡,填入扫描器标识,选择匹配域,点击添加按钮即可。如下图所示。

扫描器标识组	扫描器标识				
扫描器标识				每页显示 20 💌 条,当前	1第1/2页 🖾 [1] 2 ₽ 🕅
扫描器标识特	征: scanner	匹酉讨或: URL	▼ 添加		
请选择搜索条	キ 🗾 等于	User-Agent Request-Headers	查询		
序号	选择	扫描器标识特征	匹雷动	类型	操作
1		metis	User-Agent	默认	
2		bilbo	User-Agent	默认	
3		n-stealth	User-Agent	默认	
4		black widow	User-Agent	默认	

图 6-12 新建扫描器标识

匹配域,指对标识进行检测的位置:

- > User-Agent: http 报头中 User-Agent 字段的值
- ▶ URL:请求 URL,例如/webapp/showrun
- > Request-Headers: http 报头中所有请求头(包括报头名和报头值)

6.5.6 删除扫描器标识

点击扫描器标识右侧【 1 发钮,即可删除无用的扫描器标识。

↓ 只能删除自定义扫描器标识,如需删除多个,请勾选多个后,点击删除所选按钮。

第7章 **缺省规则**

7.1 规则管理

该章对 WAF 的缺省规则进行管理

缺省规则分为如下图的3类。

缺省规则	管理						每〕
规则分类	: 全部 🔻 规则	ID:	查询	◎检测	◉阻斷	启用	
序号	1全部 HTTP 筆略	规则分类	规则描述				阶段
1	XSS攻击 SOL XX	http-policy	Method is not allowed by policy				请求头
2		http-policy	Request content type is not allowed by policy				请求头
3	960034	http-policy	HTTP protocol version is not allowed by policy				请求体
4	960035	http-policy	URL file extension is restricted by policy				请求体
5	960038	http-policy	HTTP header is restricted by policy				请求体
6	973336	xss-attacks	XSS Filter - Category 1: Script Tag Vector				请求体
7	981136	xss-attacks					请求体
8	981018	xss-attacks					请求体
9	958016	xss-attacks	Cross-site Scripting (XSS) Attack				请求体
10	958414	xss-attacks	Cross-site Scripting (XSS) Attack				请求体
11	958032	xss-attacks	Cross-site Scripting (XSS) Attack				请求体
12	958026	xss-attacks	Cross-site Scripting (XSS) Attack				请求体
13	958027	xss-attacks	Cross-site Scripting (XSS) Attack				请求体
14	958054	xss-attacks	Cross-site Scripting (XSS) Attack				请求体

可以根据分类,规则 ID 进行查询。如下图所示,查询规则为 960010 的规则

规贝	则分类:	全部	▼ 规则ID 960010	查询		◎检测	●阻断	启用			
序号	-	规则名称	规则分类	规则描述					阶段	规则级别	操作
1		960010	http-policy	Request content type is not allowed by policy					请求头	严重	详细 禁用
	缺省规	则管理							每页显示 20 ▼条,	当前第1/8页 🛛 🖓 [1] :	2345 🕅
	规则分割	类: 全部	▼ 規则ID:	查询	◎检测	◉阻断	启用				
	序号	规则名称	规则分类	规则描述				阶段	规则级别	操作	
	1	960032	http-policy	Method is not allowed by policy				请求头	严重	详细 禁用	
	2	960010	http-policy	Request content type is not allowed by policy				请求头	严重	详细 禁用	
	3	960034	http-policy	HTTP protocol version is not allowed by policy				请求体	严重	详细 禁用	
	4	960035	http-policy	URL file extension is restricted by policy				请求体	严重	详细 禁用	
	5	960038	http-policy	HTTP header is restricted by policy				请求体	警告	详细 禁用	
	6	973336	xss-attacks	XSS Filter - Category 1: Script Tag Vector				请求体	严重	详细 禁用	
	7	981136	xss-attacks					请求体	严重	详细 禁用	
	8	981018	xss-attacks					请求体	严重	详细 禁用	
	9	958016	xss-attacks	Cross-site Scripting (XSS) Attack				请求体	严重	详细自用	
	10	958414	xss-attacks	Cross-site Scripting (XSS) Attack				请求体	严重	详细 禁用	
	11	958032	xss-attacks	Cross-site Scripting (XSS) Attack				请求体	严重	详细 禁用	
	12	958026	xss-attacks	Cross-site Scripting (XSS) Attack				请求体	严重	详细 禁用	

可以对缺省规则进行启用和禁用操作,显示禁用按钮的,规则为启用状态,显示启用按钮

的,规则为禁用状态。可以使用这两个按钮进行相应的操作。

所有的单个规则设定完成以后,执行启用功能才能启用,如下图所示



云枢擎天 WEB 应用防火墙用户使用手册

规则分类:	全部	▼ 规则ID:	查询	○检测 ●阻断	Ŧ
序号	规则名称	规则分类	规则描述		_

第8章 **策略管理**

8.1 策略管理介绍

该模块是 WAF 的核心模块之一, 主要是完成 WAF 防护策略的配置, 包含如下功能

- 策略模板
- 策略管理
- 黑白名单
- 协议规范检测
- 输入参数验证
- 访问控制
- 基本攻击防护
- 盗链防护
- 爬虫防护
- 扫描防护
- 暴力浏览攻击防护
- HTTP CC 防护
- 网站隐身
- 站点转换
- 数据窃取防护
- 实时关键字防护

- 错误码过滤
- 策略生效
- 策略浏览

8.2 策略管理

策略管理用于新建、删除策略,可以修改策略中每个子模块的配置并支持批量修改,同时 集成了策略中每个子模块的状态显示,如下图所示。

每个策略都含有 16 个子模块可供配置:黑白名单、协议规范检测、输入参数验证、访问 控制、基本攻击防护、盗链防护、爬虫防护、扫描防护、暴力浏览攻击防护、HTTP CC 防护、 会话跟踪防护、网站隐身、站点转换、数据窃取防护、实时关键字防护、错误码过滤。每个防 护子模块有独立的开启和关闭配置,有3到4种防护动作可选,用户可灵活组合。

云枢擎天 WEB 应用防火墙用户使用手册

策略	管理								
P- [添加 策略名称由字母开关	头,字母、数字和	和中划线组成,长度为1到20			
	序号	选择	策略名称	子模块策略	状态	防护动作	操作		
-	1		P-web0				🛃 🛍		
				黑白名单	关闭		3		
				协议规范检测	关闭	允许	2		
				输入参数验证	关闭	允许			
				访问控制	关闭		2		
				基本攻击防护	关闭	阻止			
				盗链防护	关闭	允许			
				爬虫防护	关闭	允许			
				扫描防护	关闭	允许			
				暴力浏览攻击防护	关闭	允许			
				HTTP CC防护	关闭	允许	2		
				会话跟踪防护	关闭	允许			
				网站隐身	关闭				
				站点转换	关闭				
				数据窃取防护	关闭	隐藏	2		
				实时关键字过滤	关闭	请求关键字过滤: 阻止, 应答关键字过滤: 隐藏			
				错误码过滤	关闭		2		
+	2		P-web1				🗗 🖬		
会讲	>14. 🗌 明明(完全)括73年								

图 8-1 策略管理

8.2.1 添加策略

在顶部策略名称栏中输入策略名称,点击【添加】按钮即可添加新策略,如下图所示。策略名称由字母开头,字母、数字和中划线组成,长度为1到20。

策略管理	
P- olicy6	添加 刪除

图 8-2 添加策略

8.2.2 删除策略

对于已添加的策略,可以点击策略右侧【 1 发钮进行删除,也可在左侧勾选多个策略, 点击【删除】,如下图所示。



云枢擎天 WEB 应用防火墙用户使用手册

策略管理 · · · · · · · · · · · · · · · · · · ·								
P-web2 添加 策略名称由字母开头,字母、数字和中划线组成,长度为1到20								
	序号	选择	策略名称	子模块策略	状态	防护动作	操作	
+	1	V	P-web0				🛃 🛅	
+	2		P-web1				🛃 🖬	
全选	全选 🖵 删除所选							

图 8-3 删除策略

记经与服务绑定的策略无法直接删除,须与服务解除绑定后再删除。解除绑定方法详见服务管理章节。

8.2.3 编辑策略

点击策略名右侧对应的编辑按钮,进入该策略的批量编辑页面。如下图所示。

批量编辑页面提供 16 个子模块的开启关闭选择、防护动作选择等功能,用户可根据自己的需要批量设置策略中的各个子模块。

—些模块仅仅选择开启状态并不能有效防护,需要进一步配置该模块的防护参数,配置方法见相关章节。
编辑策略		
策略名称: P-web0		
	状态	防护动作 策略状态开启后,请查看是否已经配置相关防护数据, 使防护生效
黑白名单:	C _{开启}	
协议规范检测:	C _{开启}	允许 💌
输入参数验证:	C _{开启}	允许 💌
访问控制:	C _{开启}	
基本攻击防护:	C _{开启}	国山
盗链防护:	C _{开启}	允许 🔽
爬虫防护:	C _{开启}	允许 🔽
扫描防护:	C _{开启}	允许 💌
暴力浏览攻击防护:	C _{开启}	允许 🔽
HTTP CC防护:	C _{开启}	允许 🔽
会话跟踪防护:	C _{开启}	允许 🔽
网站隐身:	C _{开启}	
站点转换:	C _{开启}	
数据窃取防护:	C _{开启}	隐藏
实时关键字过滤:	C _{开启}	请求关键字过滤: 阻止 💌 应答关键字过滤: 隐藏 💌
错误码过滤:	^C 开启 [€] 关闭	
	ζ μ	前定 取消

图 8-4 批量编辑策略

8.3 策略模板

策略模板,用于预定义新添加策略中各模块默认的"开启"和"关闭"状态,如下图所示。 选择"开启"和"关闭"状态后,点击确定即可保存。

修改这里并不能直接控制已有策略中各个子模块的开启关闭状态,而会影响之后新建的策略中个子模块的开启关闭状态。

默认为关闭状态的模块,大多还需要进一步配置该模块的防护参数才能更好的防护,配置 方法见相关章节。

SPENDIEUX			
默认策略模板配置			
	●全部开启	C 全部关闭	策略模板,定义新添加策略中各模块默认的开启和关闭状态
黑白名单:	C _{开启}	◎关闭	
协议规范检测:	●开启	C _{关闭}	
输入参数验证:	O _{开启}	●关闭	
访问控制:	O _{开启}	€关闭	
基本攻击防护:	●开启	○关闭	
盗链防护:	●开启	○关闭	
爬虫防护:	●开启	○关闭	
扫描防护:	◙开启	○关闭	
暴力浏览攻击防护:	C _{开启}	●关闭	
HTTP CC防护:	C _{开启}	●关闭	
会话跟踪防护:	C _{开启}	●关闭	
网站隐藏:	C _{开启}	●关闭	
站点转换:	C _{开启}	●关闭	
数据窃取防护:	C _{开启}	●关闭	
实时关键字过滤:	C _{开启}	◎关闭	
错误码过滤:	C _{开启}	●关闭	
			确定 重置

图 8-5 策略模板

8.4 黑白名单

黑白名单提供一套全局请求检测机制,目前支持的检测域有 IP, IP 段, URI, COOKIE 名称, COOKIE 值, COOKIE 名称和值,查询参数名称,查询参数值,查询参数名称和值,表单参数名称,表单参数值,表单参数名称和值,Referer 头域,共13种。支持的检测方法有字符 串匹配和正则匹配。如果请求中对应检测域中数据与黑名单中规则匹配,则禁止该请求;如果 请求中对应检测域中数据与白名单中规则匹配,则允许该请求通过,并跳过后续所有针对请求 的防护模块。

配置界面如下图所示,可在顶部策略名称下拉菜单中选择要编辑的策略。

云枢擎天 WEB 应用防火墙用户使用手册

黑白	自名单					
策略	名称: P-default	•				
	黑白名单 状态:	● 开启 ○ 关闭				选择是否开启黑白名单检 测。推荐: 是。
	类型	黑白名单种类	匹配模式	值	操作	用于全局的访问检测,黑名单优先级高于白名
	黑名单	IP 🔹	字符串匹配 ▼		添加	半; 在黑名单或白名单中,规则的页面显示顺序即
	白名单	表单参数名称和值	正则匹配	wlpf\s+name=wlpf\s+v	Ť	其检测顺序;
	白名单	表单参数名称和值	字符串匹配	wlpfname=value	Ű	IP的配置格式如: 1.2.3.4; IP段的配置格式如: 1.2.3.4-1.2.3.6;
	白名单	表单参数值	正则匹配	wlpf\s+valueonly	Ű	其他项检测值支持中英文输入,最大长度512
	白名单	表单参数值	字符串匹配	wlpfvalue_name	Ť	字符
	白名单	表单参数名称	正则匹配	wlpf\s+nameonly	Ũ	
	白名单	表单参数名称	字符串匹配	wlpfname-value	Ű	
	白名单	查询参数名称和值	正则匹配	\bwlqs\b.*\bname\b=\	Ű	
	白名单	查询参数名称和值	字符串匹配	wlqs)name=value	۳ ۳	
	白名单	查询参数值	正则匹配	\bwlqs\b.*value\d{3}	۵.	
	白名単	查询参数值	字符串匹配	wlquerystring(value	۳	

图 8-6 黑白名单配置界面

↓ 黑名单优先级高于白名单, 黑名单或白名单内部按照添加时的顺序进行匹配。

8.4.1 添加黑白名单

依次选择类型、黑白名单种类、匹配模式,填入匹配表达式或值,点击【添加】,最后点击 底部的【确定】按钮即可保存,如下图所示。



黒	黑白名单							
策略	名称: P-L3	•						
	黑白名单							
	状态:	● 开启 ◎ 关闭						
	类型	黑白名单种类	匹配模式	值	操作			
	黑名单 🔻	COOKIE值 -	正则匹配 🔻	\d{4,}blcookiename	添加			
	黑名单	COOKIE值	正则匹配	\d{4,}blcookiename	Ű			
				确定重置				

图 8-7 添加黑名单

8.4.2 删除黑白名单

点击每条黑白名单右侧的【 🇯 】按钮, 并点击底部【确定】按钮即可实现删除。

8.4.3 开启和关闭

若要黑白名单开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态可以 独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。如下图所示。



黑白	自名单				
策略	名称: P-L3	•			
	黑白名单				
:	状态:	◎ 开启 ● 关闭			
	类型	黑白名单种类	匹配模式	值	操作
	黑名单 🔻	COOKIE值 -	正则匹配 🔻	\d{4,}blcookiename	添加
	黑名单	COOKIE值	正则匹配	\d{4,}blcookiename	۲.
				确定重置	

图 8-8 开启和关闭

8.5 协议规范检测

协议规范检测用于限制 http 请求头和请求体中各组成元素的长度或个数,实现有效阻断缓 冲溢出等攻击。如果请求中有超过限制的数据,则按照防护动作生效。

配置界面如下图所示。

云枢擎天 WEB 应用防火墙用户使用手册

1. 治坦芬检测	
ル区飛び日短期	

嚻名称: P-default	•			
协议规范性检验				
状态:	● 开启 ● 关闭	开启对HTTP协议各组成元素的长度限制功能。这些检查能够有效阻断缓冲溢出等攻击。要关闭单个检测,在参数栏中留空。推荐:是		
请求头域值的最大长度:	512	定义请求报头值的最大长度。推荐: 512		
请求头名称的最大长度:	64	定义报头名字的最大长度。推荐:64		
请求头域的最大个数:	20	定义了一个请求能够包含的最多报头个数。推荐:20		
请求体的最大长度:	32768	请求body的最大长度。POST请求有一个包含表单参数和值的请求body。推荐:32768		
表单参数值的最大长度:	512	指定表单参数值的最大长度。推荐: 512		
表单参数名称的最大长度:	600	指定表单参数名字的最大长度。推荐:64		
请求行的最大长度:	4096	请求行是请求中的第一行。包括Method、URL和HTTP版本。最大请求行长度应该与最大URL长度近 似。		
查询参数值的最大长度:	256	定义请求报头值的最大长度。推荐: 512		
查询参数名称的最大长度:	32	指定参数名字的最大长度。推荐:64		
查询参数的最大个数:	16	查询参数的最大个数。推荐:40		
禁止的请求协议:	HTTP/0.9,HTTP/1.0	指定禁止的请求协议(HTTP/0.9,HTTP/1.0,HTTP/1.1),多项配置以半角逗号分隔		
COOKIE最大个数:	30	所有的Cookie可以被包含在一个"Cookie:"首部中(格式为name=value,以半角分号隔开)。 此选项限制了cookie的数量。推荐:40		
禁止的方法:	connect,options,delete,	指定禁止的HTTP方法,多项配置以半角逗号分隔		
禁止的HOST:	www.deny.com	指定禁止的host,多项配置以半角逗号分隔		
防护动作。				
动作:	阳止	防护动作可以选择允许(允许继续请求服务器资源),阻止(阻止请求,返回403页面,或,相应的 错误过滤页面),重定向(重定向请求到配置的重定向URL),阻断(在设置的阻断时间内,阻止同 源IP的请求)。		

图 8-9 协议规范检测配置界面

目前支持对如下字段进行规范检测:

- > 请求头域值的最大长度 指定请求报头值的最大长度
- > 请求头名称的最大长度 指定报头名字的最大长度
- ▶ 请求头域的最大个数 指定一个请求能够包含的最多报头个数

> 请求体的最大长度 – 指定请求体 body 的最大长度(POST 请求有一个包含表单参数值

和名称的请求 body)

- > 表单参数值的最大长度 指定表单参数值的最大长度
- > 表单参数名称的最大长度 指定表单参数名字的最大长度
- ▶ 请求行的最大长度 指定请求行的最大长度。请求行时请求中的第一行,内容包含 Method、URL 和 HTTP 版本,例如: GET / index.php HTTP/1.1。设定的最大请求行长度应 接近与最大 URL 长度。

- 查询参数值的最大长度 指定查询参数值的最大长度。查询参数在 URL 中以如下形式 出现: "search.php?queryname1=queryvalue1&queryname2=queryname2&…",其中 queryname=queryvalue 的组合是为一组查询参数,等号前 queryname 为查询参数名称, 等号后 queryvalue 为查询参数值。
- > 查询参数名称的最大长度 指定查询参数名称的最大长度, 推荐 64 字节。
- ▶ 禁止的请求协议 指定禁止的 HTTP 请求协议类型,包括 HTTP/0.9, HTTP/1.0, HTTP/1.1 三种,多项配置以半角逗号分隔。默认值为空,即忽略该项检测。
- COOKIE 最大个数 指定请求头中包含 cookie 的最大个数,推荐 40 个。请求首部中, cookie 的格式为 "Cookie:name1=value1,name2=value2,…",这里一个 name=value 形式的 组合,视为一个 cookie。
- ▶ 禁止的方法 指定禁止的 HTTP 请求方法,多项配置以半角逗号隔开,默认值为空。HTTP 的请求方法包括: GET/POST/HEAD/PUT/DELETE/TRACE/CONNECT/OPTIONS 等。
- ▶ 禁止的 HOST 指定禁止的请求头中的 HOST 头域,多项配置以半角逗号隔开,默认值 为空。HOST 头域形如: 192.168.1.1:8080 或 www.example.com。

注:对于非数值类的输入项(禁止的请求协议、禁止的方法、禁止的 HOST),如果不填入数据,则代表不进行检测,如果填入多项数据,使用半角逗号分开;对于数值类的输入项,必须填入数值。

8.5.1 配置阈值

在检测域对应的输入框内输入数据,选择防护动作,点击确定即可保存。

8.5.2 防护动作

防护动作包含:允许,阻止,重定向,阻断共四种。如果某请求与规则匹配,则触发防护 动作。

允许:允许该请求通过,并记录日志。

阻止:阻止该请求通过,返回 403 页面或对应的错误过滤页面,并记录日志。

重定向:将该请求重定向至指定 URL。

阻断:阻止第一个匹配规则的请求,并在之后的一段时间内,阻止该源 IP 的所有请求。

8.5.3 配置例外

例外旨在为可能存在的误报提供解决方法,如果一个正确的请求被识别为攻击,则可以通 过配置例外跳过本模块的检测。

目前支持例外配置的模块有协议规范检测、暴力浏览攻击防护、会话跟踪防护。

选择例外检测域、匹配方式,填入例外检测域值;点击添加按钮,点击确定保存即可。配 置界面如下图所示。

例外检测域: IP、IP 段、HOST、REFERER、URL、User-Agent。

匹配方式:字符串匹配、正则匹配。

例外检测值:由用户自定义。

云枢擎天 WEB 应用防火墙用户使用手册

例外检测域	匹配方式	例外检测值	操作	
IP	▼ 字符串匹配	•	添加	
User-Agent	字符串匹配	welcome-user-bgent	Ű	-
User-Agent	正则匹配	(requester clawer ro	Ű	
URI	正则匹配	(welcome test)piuri	Ű	
URI	字符串匹配	welcomeuri	Ű	- 自己的가致痛,不过110%%%2位测
REFERER	正则匹配	(pass skip)\.pi\.ref	Ű	
REFERER	字符串匹配	http://avoid.pi.refe	Ű	
HOST	正则匹配	^rx\.pi\.com\$	Ű	-
HOST	字符串匹配	str.pi.host.com	Ű	

图 8-4 例外配置界面

8.5.4 开启和关闭

若要协议规范检测开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态 可以独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.6 输入参数验证

输入参数验证提供两个功能:参数验证和上传文件格式检查。

参数验证:用于对 http 请求中携带的参数进行验证,如果请求中携带的参数与定义的规则 匹配,防护动作生效。

上传文件格式检测:检测向网站上传的文件是否为伪造,若为伪造,则禁止其上传。

8.6.1 配置参数验证

配置界面如下图所示。



创建参数

云枢擎天 WEB 应用防火墙用户使用手册

(型	匹配方式	匹配表达式	操作
查询参数名科▼	正则匹配 👻		添加
表单参数名和参 数值	正则匹配	pvpf.+name=pvpf.+val	Ű
表单参数名和参 数值	字符串匹配	pvpfname=pvpfvalue	Ű
表单参数值	正则匹配	pvpf[^uiop]+value	Ű
表单参数值	字符串匹配	pvpfvalue	Ű
表单参数名称	正则匹配	pvpf\d+name	Ű
表单参数名称	字符串匹配	pvpfname	Ű
查询参数名和参 数值	正则匹配	pvqsname\d{2}=pvqsna	Ű
查询参数名和参 数值	字符串匹配	pvqsname=value	Ű
查询参数值	正则匹配	pvqsname[xyz]{2}only	Ű
查询参数值	字符串匹配	pvqsvalue>str	Ű
查询参数名称	正则匹配	pvqsname\d{2}only	Ű
查询参数名称	字符串匹配	pvqsname	Ű

图 8-5 参数验证配置界面

添加操作:选择参数类型、匹配方式,填入匹配表达式,点击添加,点击确定,即可保存。

- 类型 指定创建参数的类型,包含查询参数名称、查询参数值、查询参数名和参数值、 表单参数名称、表单参数值、表单参数名和参数值。
- > **匹配方式** 指定参数匹配的方式, 支持正则匹配和字符串匹配。
- **匹配表达式** 指定需匹配的参数表达式,表达式支持中英文字符,大小写敏感,最长 允许输入 32 字符。
- 操作 添加或删除所创建的参数。删除操作:点击指定行后的【¹】按钮,点击确定即可。

8.6.2 防护动作

防护动作包含:允许,阻止,重定向共三种。如果某请求与规则匹配,则触发防护动作。 允许:允许该请求通过,并记录日志。 阻止:阻止该请求通过,返回 403 页面或对应的错误过滤页面,并记录日志。

重定向:将该请求重定向至指定 URL。

8.6.3 开启和关闭

若要输入参数验证开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态 可以独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.7 访问控制

访问控制用于控制网站中的特定路径或文件的访问。

8.7.1 配置访问控制

填入默认初始页面,选择访问资源类型,填入值,点击添加,点击确定,即可保存。配置 界面如图所示。

初始石盂过速			
初新贝面过来 状态: 默认初始页面:	◎ 开启 ◎ 关闭 forum.php		选择是否开启访问控制。推荐:是。 例如:http://www.example.com/index.html或/index.html,大小写敏感。
访问资源类型	值	操作	用户访问允许的入站页面时,允许其访问;用户访问禁止目录或禁止页面时,跳转到默认初始页面
允许的入站页面	-	添加	该列表配置内容大小写敏感,最大长度为512
允许的入站页面	/css_tutorials/050_p	Ť	
禁止访问文件	css_tutorials/001_CS	ŵ	
禁止访问目录	1/admin	Ŵ	
禁止访问文件	misc.php	Ű	

图 8-6 访问控制配置界面

默认初始页面:网站的首页,任何人均可访问的页面。当一个 web 用户首次访问网站时,

会被重定向至默认初始页面。对于非首次访问的请求,则不会重定向。



访问资源类型:

允许的入站页面-允许任何用户访问的页面。

禁止访问的文件-禁止任何用户访问的页面,形如/path/page.html;如果请求访问该资源,则重定向至默认初始页面。

禁止访问的路径-禁止任何用户访问的路径,形如/path1/path2,如果配置,则该路径下的所有文件均不可访问。如果请求访问该路径或该路径下的资源,则重定向至默认初始页面。

8.7.2 开启和关闭

若要访问控制开始生效,须将其整为开启状态。每个策略的子模块开启与关闭状态可以独 立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.8 基本攻击防护

基本攻击防护,内置强大的默认防护规则,用于防护常见的 web 攻击 (例如 sql 注入攻击、 跨站脚本攻击、操作系统命令注入、远程文件包含、目录遍历攻击等),同时支持用户自定义规则,可对 http 请求对灵活的限制。

8.8.1 默认规则库

默认规则库可以通过规则库升级来更新,建议及时更新至最新版本。升级方法详见规则库 升级章节。

8.8.2 新建自定义规则

 URI 匹配:填写规则名称,在 URI 匹配输入框中输入要匹配的字符串,点击添加,点击确 定,即可保存。配置界面如下图所示。



创建自定义规则 🔺		
规则名称:	basicuri	规则名称用于识别自定义规则,最大长度为32
URI匹雷:	basicuri	对URI进行字符串匹配,大小写不敏感。如配置'/*', 表示不对URI进行检测,最大长度为 512。
高级匹配:	/*	用于配置HTTP请求头域的检测规则,大小写不敏感
		添加

图 8-7 新建 URI 匹配规则

2. 高级匹配:填写规则名称,点击高级匹配编辑按钮 🔀,选择检测域,选择匹配方式,

填写数值,点击插入-应用-添加,点击确定即可保存。配置界面如下图所示。

创建自定义规则 🔺		
规则名称:	Hexpress1	规则名称用于识别自定义规则,最大长度为32
URI匹酉:	/*	对URI进行字符串匹配,大小写不敏感。如配置, 512。
高级匹配:	/*	用于配置HTTP请求头域的检测规则,大小写不曼
高级匹配设置 匹配表达式: 检测域: 匹配方式: 数值: 串联关系:	/* URI ▼ 〒则匹配: ● 与 ◎ 或 插入 应用 取消	
		添加

图 8-8 新建高级匹配规则

检测域: 支持客户端 IP、URI、参数、Method (方法)、HTTP-VERSION (HTTP 版本)、HEADER (请求头域)。

匹配方式:支持字符串匹配、字符串不匹配、正则匹配、正则不匹配四种方式;根据检测域不同,可能略有差别。字符串不匹配和正则不匹配是一种在字符串匹配和正则匹配基础上取反的匹配方式。

数值:用于匹配的表达式或者字符串。

串联关系:高级匹配支持将多个独立的表达式用'与'、'或'串联起来,组成更复 杂的表达式。在数值中输入一个独立的表达式,选择串联关系并点击插入,然后再 填写下一个表达式;当整个表达式填写好后,点击应用-添加,点击确定即可保存。

注 1: URI 匹配和高级匹配同时填写与分别填写没有区别,可独立生效

注 2: 匹配表达式默认为/*代表不匹配任何内容

8.8.3 查看自定义规则

自定义规则列表中,保存了当前的自定义规则。如果表达式过长,可将鼠标焦点移至表达 式出,会弹出显示框,用于完整显示表达式,方便用户检查表达式、复制表达式。

定义规则列表 🔺					
规则名称	启用	URL匹配	高级匹配	操作	
argAipOhp1Aopen	是	/*	(Argument rx (preg_r	ш	
riAcookieOuri	是	/*	(Argument rx (preg_repl	ace popen fopen sy	sopen compile pas
rior	是	/*	(\s \+)*1(\s \+)*=(\s \+))*1(\s \+)*-{2,})	.are[(+(5] , @)a
ddffsdfd	是	/*	(URI rx script(\+AD[Ű	
ıriAparamAcookie	是	/*	(URI rx (fork exec s	Ű	
a2	是	/*	(HEADER User-Agent s	ũ	
a	是	/*	(HEADER User-Agent s	Ű	
trandrx	是	/*	(URI nstr bastruri)	Ű	
trand	是	/*	(IP nstr 8.8.8.8) an	Ű	
astruri	是	bastruri	/*	Ť	

图 8-9 自定义规则列表

8.8.4 删除自定义规则

点击规则右侧的【 🇯 】按钮, 并点击底部【确定】按钮即可实现删除。

8.8.5 防护动作

防护动作包含:允许,阻止,重定向,阻断共四种。如果某请求与规则匹配,则触发防护 动作。

允许:允许该请求通过,并记录日志。

阻止:阻止该请求通过,返回 403 页面或对应的错误过滤页面,并记录日志。

重定向:将该请求重定向至指定 URL。

8.8.6 应答体检测

黑客可能通过 web shell 和其他手段, 试应答中包含一些系统相关的敏感信息。应答体防护 旨在防护异常的应答体内容, 如果应答体中匹配了防护规则, 则阻止该应答, 客户端不会收到 任何应答体。

应答体检测开关配置如下图所示。勾选启用点击确定即可生效。

应答体检测 🔺	
状态:	☑ 启用

图 8-10 应答体检测配置

应答体检测开启后, web 服务的安全性会显著提高, 但理论上会损失一定性能, 这里请用 户灵活选择。

8.8.7 开启和关闭

若要基本攻击防护开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态 可以独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.9 盗链防护

盗链防护能有效防护恶意站点的盗链行为,节约本站流量。盗链防护使用基于 Referer 的防护算法,除允许入站页面外,只允许带有合法 Referer 的请求通过,若请求中含有非法的 Referer 或没有 Referer,则认为是盗链行为,触发防护动作。

8.9.1 配置盗链防护

允许入站页面:无需合法 Referer 也能访问的页面,一般配置为网站的合法入口。必填项, 如果不配置,可能导致网站无法访问。

Referer URL: 合法的 Referer,可简单理解为本站域名和子域名,例如 www.test.com, blog.test.com; 也可以配置为完整 Referer 信息,如 http://www.test.com。



云枢擎天 WEB 应用防火墙用户使用手册

经销防护			请将面	雷项填写完整,否则防护不生效。
略名称: P-web1	•			
盗锚防护				
状态:	● _{开启} [●] 关闭			
防护算法:	Referer防护			
允许入站页面:	/index.html /welcome.jsp /default.php /cgi-bin/user?action=login	×	填写 [;] http 应填 确,; 符(;	相对url,例如:页面 ://www.test.com/index.html 写/index.html,填写应完整、准 大小写敏感,可填多个,用回车 换行)分隔。最大长度2000字符
Referer URL:	www.test.com www.friend.com	×	例如 用回: 200 (: www.example.com URL之间 车符(换行)分隔;最大长度 0字符
防护动作 🔺				
动作:	<u>BH1F</u>		防护 求 返 面 重 时	动作可以选择允许(允许继续请 务器资源),阻止(阻止请求, 403页面,或,相应的错误过滤页 ,重定向(重定向请求到配置的 句URL),阻断(在设置的阻断 内,阻止同源IP的请求)。
例外 🔹				
例外检测域	匹配方式	例外检测值	操作	配置例外数据,不进行盗链防护
IP	▼ 字符串匹配 ▼		添加	检测
		确定 重置		

图 8-11 盗链防护配置

8.9.2 防护动作

防护动作包含:允许,阻止,重定向共三种。如果某请求与规则匹配,则触发防护动作。

允许:允许该请求通过,并记录日志。

阻止:阻止该请求通过,返回 403 页面或对应的错误过滤页面,并记录日志。

重定向:将该请求重定向至指定 URL。

8.9.3 配置例外

见协议规范检测章节-例外配置。

8.9.4 开启和关闭

若要盗链防护开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态可以 独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.10 爬虫防护

爬虫防护能有效防护互联网中的恶意爬虫,可屏蔽特定的搜索引擎爬虫节省带宽和性能, 也可屏蔽扫描程序爬虫,避免网站被恶意抓取页面。

8.10.1 配置爬虫防护

爬虫防护的配置依赖于爬虫标识组,爬虫标识组的配置与组织详见对象库-爬虫标识组章 节。

选择需要防护的爬虫标识组、选择防护动作点击确定即可保存。配置界面如下图所示。

爬虫防护		
策略名称: P-web0	-	
爬虫防护		
状态:	●开启 C关闭	
爬虫标识组:	DefaultRobots	爬虫标识组为在对象库中爬虫标识组中定义的,作为爬虫防护的 对象。
防护动作 🔺	groupi	
动作:	MIL	防护动作可以选择允许(允许继续请求服务器资源),阻止(阻 止请求,返回403页面,或,相应的错误过滤页面),重定向 《重定向请求到赋置的重定向URL》,阻断(在设置的阻断时间 内,阻止同源IP的请求)。
	确定 重置	

图 8-19 爬虫防护配置

8.10.2 防护动作

防护动作包含:允许,阻止,重定向共三种。如果某请求与规则匹配,则触发防护动作。 允许:允许该请求通过,并记录日志。

阻止:阻止该请求通过,返回 403 页面或对应的错误过滤页面,并记录日志。

重定向:将该请求重定向至指定 URL。

8.10.3 开启和关闭

若要爬虫防护开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态可以 独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.11 扫描器防护

8.11.1 配置扫描器防护

扫描器防护的配置依赖于扫描器标识组,扫描器标识组的配置与组织详见对象库-扫描器标识组章节。

选择需要防护的扫描器标识组、选择防护动作点击确定即可保存。配置界面如下图所示。

扫描防护		
策略名称: P-web1	•	
扫描防护		
状态:	€ _{开启} C _{关闭}	
扫描器标识组:	DefaultScanners	扫描器标识组为在对象库中扫描器标识组中定义的,作为扫描防 护的对象。
防护动作 🔺	groupi	
动作:	PELL	防护动作可以选择允许(允许继续请求服务器资源),阻止(阻止请求,返回403页面,或,相应的错误过速页面),重定向(重定向请求到配置的重定向URL),阻断(在设置的阻断时间内,阻止同源IP的请求)。
		确定 重置

图 8-12 扫描器防护配置

8.11.2 防护动作

防护动作包含:允许,阻止,重定向,阻断共四种。如果某请求与规则匹配,则触发防护 动作。

允许:允许该请求通过,并记录日志。

阻止:阻止该请求通过,返回 403 页面或对应的错误过滤页面,并记录日志。

重定向:将该请求重定向至指定 URL。

8.11.3 开启和关闭

若要爬虫防护开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态可以 独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.12 暴力浏览攻击防护

暴力浏览攻击防护可有效防护某源 IP 在短时间内的大量恶意请求。同时支持例外配置。

8.12.1 配置暴力浏览攻击防护

填入单 IP 允许的最大请求数,选择防护动作,点击确定即可保存。配置界面如下图所示。

暴力浏览攻击防护				请将配置项填写完整,否则防护不生效。
策略名称: P-test	T			
暴力浏览防护 状态:	◎开启	●关闭	选择是否开启暴力浏览防护。	
单IP允许的最大请求数:	1000		请求计数的最大值,计数满足最大值时,将执行已配置的防护动作,数值范围: 1-32767	
防护动作 ^				
动作:	阳止	٣	防护动作可以选择阻止(阻止请求,返回403页面,或,相应的错误过滤页面)。	
			确定。重责	

图 8-13 暴力浏览攻击防护配置界面

单 IP 允许的最大请求数:一个源 IP 可以访问被保护服务的最大请求数,如果超过该请求数则触发防护动作。

8.12.2 防护动作

防护动作包含:阻止

8.12.3 开启和关闭

若要基本攻击防护开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态 可以独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.13 HTTP CC 防护

HTTP CC 防护提供了另外一种防止暴力浏览的防护方式,用于 CC 防护。

8.13.1 配置 HTTP CC 防护

HTTP CC防护			请将配置项填写完整,否则防护不生效。			
策略名称: P-test	¥					
状态:	●开启 ○关闭	选择是否开启CQ防护。				
最大请求数:	1000	请求计数的最大值,计数满足最大值时,将执行已配置的防护动作,数值范围:1-32767				
防护动作 ^ 动作:	問止▼	防护动作可以选择阻止(阻止请求,返回403页面,或,相应的编码过滤页面)。				
确定 重要						

图 8-14 CC 防护配置界面

最大请求数:可以访问被保护服务的最大请求数,如果超过该请求数则触发防护动作

8.13.2 防护动作

防护动作包含:阻止。

8.13.3 开启和关闭

若要 CC 防护开始生效,须将其调整为开启状态。每个策略的子模块开启与关闭状态可以 独立配置,选择开启或关闭状态后,点击底部【确定】按钮即可保存。

8.14 网站隐身

通过合理配置网站隐身,可以隐藏 HTTP 应答头中的指定报头,例如服务器名称、版本等 重要信息。

网站隐身配置页面如下图所示:

内城協身 策略名称: P-celue の は 的 自	e 🔽		
大态: 过滤报头 Server	 开启 选项 添加 位 	 ● 关闭 	选择是否过滤响应中的特定报头。 将删除来自服务器确的HTTP中相应报头。包括带有服务器类型信息、质本信息的报头。推荐:Server。输入报头需 以字母开头,可包含中划线或数字,最大长度32个字符,大小写不敏感,不支持对如下过滤或转换操作: Transfer-Encoding, Connection。
			确定 重量

图 8-15 网站隐身界面

推荐配置:

Date Server X-Powered-By

8.15 站点转换

站点转换页面如下图所示,可以配置规则对客户端和服务器端的请求包头或者响应报头进行修改或删除,隐藏其真实的数据信息。动作中分别有:重写请求报头、删除请求报头、重写URL、重写响应报头、删除响应报头。配置需要修改或删除的报头匹配值,并选择相应的动作,选择添加按钮即可配置成功。

如要删除,则直接点击每条规则对应行后的⁶⁶,即可将该站点转换规则删除。

站点转	考换					
策略名	称: P-celue	\checkmark				
, j	点转换					
1+1	* .		选择是否开启站点转换功			
1	. L.					(1)200 (1
站。	点转换列表 🔺					
1	規則名称	动作	匹配值		洗項	用于重写,删除诸求报头和应答报头、重
						写URL。重写报头,如果报头存在,则编
ŀ	аааа	删除响应报头 🛛 💟	Server	dgag	添加	辑报头,如果报头不存在,则插入报头,
a	аааа	删除响应报头	Server		Ť	不支持对如下过滤或转换操作:
	aaa	重写响应报头	DATE	doao	ш	Transfer-Encoding, Connection.
l F						
a	за	里与请求损失	UA-CPU	sdlgj	Ψ.	
				确定	重置	

图 8-16 站点转换配置界面

8.16 数据窃取防护

数据窃取防护页面如下图所示,可以在该页面配置受保护数据,返回给用户的数据如果与 设置的保护数据相匹配,将匹配的数据用"XXXX"字符进行隐藏。选择配置方式以及保护数据, 点击添加即可配置成功。

如要删除,则直接点击每个保护数据对应行后的40,即可将该保护数据删除。



数据窃取防护配置			
犬态:	○开启	●关闭	选择是否过滤响应中的保护数据。
护动作 🔨			
力作:	隐藏	~	选择隐藏,返回给客户端的数据如果与设置的保护数据匹配,将匹配的数据用"XXXX"字符进行隐藏
保护数据 🔺			
匹配方式	保护数据	选项	保护数据为数据窃取防护检测的数据特征,支持中英文及可显示字符, 字母匹配大小写敏感,数据最多32
正则匹配 🔽	法轮功	添加	将
正则匹配	法轮功	Ť	
字符串匹配	游行示威	Ű	
字符串匹配	革命	fiir	

图 8-17 数据窃取防护界面

8.17 实时关键字过滤

关键字配置界面如下图所示,用户输入关键字列表,多个关键字用"|"隔开,选择防护动

作,保存即可。一旦应答中含有关键字,触发防护动作。

应答关键字过滤 🔺		
gzip压缩:	区支持	是否支持gzip压缩的应答体检测。
MIME <u>类型</u> :	☑ text/html ☑ text/css ☑ text/xml □其他	根据需要增加过滤的MIME类型,可输入多 个,用半角的逗号(即英文逗号)分隔,最 大长度100字符
动作:	隐藏	隐藏:返回给客户端的数据如果与设置的应 答关键字匹配,将匹配的数据用 [*] XXXX"字符 进行隐藏;阻止:阻止请求,返回空页面。
	*	可输入多个关键字,最大长度500字符,多 关键字以门分隔。关键字中可包含空格,并 至少包含一个中英文字符,注意空格的使用

图 8-18 应答关键字配置

防护动作,指一旦发现关键字之后 WAF 采取的动作:

- > 隐藏: 隐藏网页中的关键字, 使用 XXXX 代替关键字, 并记录日志
- > **允许:**不对关键字做处理,只是记录日志,相当于审计功能

关键字默认防护 text/html, text/css, text/xml 三种 MIME 类型的应答,如果用户需要防护 其他类型的应答,可以勾选其他,填入自定义的 MIME 类型。

关键字默认开启"支持 gzip 压缩"默认,如果用户网站使用 gzip 压缩,建议开启该选项。 如果不勾选,将无法对 gzip 压缩的应答做关键字过滤。

8.17.1 关键字白名单

如果关键字过滤出现误报,可以设置关键字白名单防止误报,配置界面如下图所示。

实时关键字过滤白名单列表	^

添加方式	关键字	关键字类型	URL	匹配模式	操作	配置实时关键字过滤白名单数据。
	关键字2	请求关键字 💌	/page2.html	正则匹配 🔽	添加	大罐子名称阎孟:文持中央义阎孟,取大长度 30字符;匹配模式选择"字符串匹配"时,可输
自定义	关键字2	请求关键字	/page2.html	正则匹配	Ű	入多个关键字,多关键字以十分隔,关键字中
自定义	关 键字 1	应答关键字	/page1.html	字符串匹配	ũ	可包含空格,并至少包含一个中英文字符,注
						ー个正则表达式。 URL配置:填写相对URL,如: http://www.test.asp/index.asp,应填写 为/index.asp,否则该白名单不生效;最大输 入长度512个字符,大小写不敏感
			确定重置			



填入关键字,选择关键字类型,填入 URL,选择匹配模式,点击添加,点击确定保存。关键字白名单配置成功后,指定 URL 中如果再次匹配该关键字,则不会触发防护动作。

8.18 错误码过滤

错误码过滤页面如下图所示,可以为每一种 HTTP 状态码映射一个页面,映射页面在对象 库-错误提示页面中定义,见相关章节。选择好 HTTP 状态码以及该状态码对应的映射页面后, 点击"添加"操作即可配置成功。

如要删除,则直接点击每个 HTTP 状态码对应行后的¹⁰⁰,即可将该映射删除。



错误码过滤			
策略名称: P-celue			
状态: 〇开	启 ③关闭		选择是否开启错误码过滤。
HTTP状态码	映射页面	操作	屏蔽服务器近回的错误提示页面,并使用自定义的返回页面。
400	default 🔽	添加	
409	default	Ű	
404	default	Ű	
403	default	Ű	
			确定 重置

图 8-19 错误码过滤配置界面

↓ IE 浏览器有"显示友好错误信息"选项,如果勾选了该选项, WAF 返回的错误页面可能不能被浏览器正确显示。



图 8-20 显示友好错误信息

8.19 策略生效

没增加或者修改一条策略,策略会自动生效。该策略生效按钮,重新加载配置策略。一般

情况下不会用到



8.20 策略浏览

查看已配置的策略集中的具体策略

用户规则协	揽				每页显示 20 ▼条,当前第1/1页 🖂 🚺 🖂
规则分类:	全部	▼ 策略名称: P-block	▼ 规则ID:	查询	
序号	规则ID	规则集	规则分类	规则描述	规则运力作
1	4100011	P-test	扫描防护	扫描防护/允许 文件内容匹配 URI 08_扫描防护_URL.data	通过
2	41220001	P-xxx	输入参数验证	输入参数验证/查询参数 字符串匹配 查询参数 111	拒绝
3	4100011	P-xxx	扫描防护	扫描防护/允许 文件内容匹配 URI 08_扫描防护_URL.data	通过
4	4100009	P-xxx	扫描防护	扫描防护/允许 文件内容匹配 请求头名字 请求头 08_扫描防护_RequestHeaders.data	通过
5	4000005	P-xxx	爬虫防护	Robots/允许 文件內容匹配 请求头:浏览器标识[UA] 07_Robots_UserAgent.data	通过
6	4100700	P-xxx	扫描防护	扫描防护/允许 文件内容匹配 请求头:浏览器标识[UA] 08_扫描防护_UserAgent.data	西
7	4100009	P-test	扫描防护	扫描防护/允许 文件内容匹配 请求头名字 请求头 08_扫描防护_RequestHeaders.data	通过
8	4100700	P-test	扫描防护	扫描防护/允许 文件內容匹配 请求头:浏览器标识[UA] 08_扫描防护_UserAgent.data	通过
9	4000005	P-test	爬虫防护	Robots/允许 文件内容匹配 请求头:浏览器标识[UA] 07_Robots_UserAgent.data	通过
10	4100009	P-block	扫描防护	扫描防护/元许文件内容匹配 请求头名字 请求头 08_扫描防护_RequestHeaders.data	通过
11	4100011	P-block	扫描防护	扫描防护/允许 文件内容匹配 URI 08_扫描防护_URL.data	通过
12	4000007	P-block	爬虫防护	Robots/deny 文件内容匹配 请求头:浏览器标识[UA] 07_Robots_UserAgent.data	通过
13	4100700	P-block	扫描防护	扫描防护/元许文件内容匹配 请求头:浏览器标识[UA] 08_扫描防护_UserAgent.data	通过

图 8-21 显示策略集信息

第9章 服务管理

9.1 透明模式服务管理

透明模式服务管理界面下图所示,该界面显示出当前已有的被保护服务信息。

服务管理	服务管理								
》 新建									
选择	状态	服务名称	服务类型	主机地址	主机端口	策略集	域名	服务直通	操作
	0	fuwu1	http	182.182.182.122	83	None		٩	a 🖓 🖓 🛍
	0	fuwu2	http	182.182.182.122	84	None		٥	a 🖓 🖓 🛍
全选 🔲	全选 🔲								



9.1.1 新建服务

下图所示:

新建服务	
*服务名称:	字母开头,字母、数字和下划线组成,长度为1到20
*服务类型:	HTTP
*主机地址:	点分十进制整数,形如: 192.168.23.4
*主机端口:	(1~65535)
域名:	
策略集:	无
MAC绑定:	□ 启用服务与MAC地址绑定
*记录访问日志:	● 是 ○否
*记录防护日志:	●是 ○否
	确定取消

图 9-2 透明模式新建服务页面

> MAC 绑定、策略集、站点域名为选填项,其它为必填项。

- ▶ 服务类型选择 HTTPS,还需要指定向浏览器提交的证书、是否验证浏览器证书、向主机提交的证书以及是否验证主机证书,证书管理参见【对象】-【证书】。
- 选择记录访问日志,则对该服务的访问均会记录在日志中,通过【日志】-【站点访问日志】可查询到相关记录。

^①在某些情况下 (如特定攻击),即使该服务选择不记录访问日志,相关访问也会记录在日志中。

9.1.2 查看服务

查看服务	
服务名称:	fuwu1
服务类型:	http
主机地址:	182.182.182.122
主机端口:	83
服务域名:	无
策略集:	None
MAC绑定:	无
记录访问日志:	记录
记录防护日志:	记录
链路绑定:	br_default
	确定

点击服务操作栏的查看按钮 🤍 可以查看该服务的所有信息, 如下图所示:

图 9-3 查看服务页面

9.1.3 修改服务

点击服务后面的修改按钮 📴 进入修改服务页面。修改服务信息修改,包括主机地址、主机



端口、MAC 绑定、策略集、站点域名以及是否记录日志。服务名称和服务类型不可以修改。

编辑服务	
*服务名称:	fuwu1
服务类型:	HTTP
*主机地址:	182.182.182.122 点分十进制整数,形如:192.168.23.4
*主机端口:	83 (1~65535)
域名:	
策略集:	无
MAC绑定:	□ 启用服务与MAC地址绑定
*记录访问日志:	◎是 ○ 否
*记录防护日志:	◎是 ◎否

确定取消

图 9-4 修改服务信息页面

9.1.4 删除服务

删除服务有两种方式,可以点击服务后面的删除按钮 fin 直接删除,也可以选择一个或多 个服务,点击【删除所选】进行删除。

9.2 反向代理模式服务管理

反向代理模式服务管理界面如下图所示,该界面显示出当前已有的被保护网络服务信息。

	皆理									
	ਡ 新建									
	序号	选择	服务名称	服务类型	虚拟地址	域名	策略集	主机地址	主机端口	操作
Ξ	1		fuwu1	http	182.182.182.141:60		None	1 (个)		🕒 🕸 🛃 🛅
								182.182.152.122	83	a 🖓 🔁 🛍
全说	全选 🔲 删除所选									



9.2.1 新建服务/主机

点击页面左上角的【^{全新建}】按钮,进入新建服务页面。在反向代理模式下,新建服务时需要输入要监控的服务名称、服务类型、虚拟地址、虚拟端口、策略集、站点域名、是否记录日志、主机地址、主机端口以及是否 SSL 连接,如下图所示:

云枢擎天 WEB 应用防火墙用户使用手册



教建版务						
*服务名称:	字母开头,字母、数字和下划线组成,长度为1到20					
*服务类型:	НТТР					
*虚拟地址:	182.182.141					
*虚拟端口:	(1~65535)					
*主机地址:	点分十进制整数,形如:192.168.23.4					
*主机端口:	(1~65535)					
域名:						
*策略集:	无					
*记录访问日志:	◎是 ◎否					
*记录防护日志:	◎是 ◎否					
*主机SSL连接:	◎是 ⑧否					
	确定 取消					

图 9-6 反向代理新建服务页面

- > 其中站点域名为选填项,其它为必填项。
- 如果服务类型选择 HTTPS,需要指定向浏览器提交的证书和是否验证浏览器证书; 如果选择 SSL 连接,需要指定是否验证服务器端的证书;同时,如果保护服务需要客 户端证书验证的话,还需要提交作为客户端的证书。
- 如果选择记录访问日志,则对该服务的访问均会记录在日志中,通过【日志】-【站点 访问日志】可查询到相关记录。

服务新建完成后,点击操作列的【³³³】按钮可以添加一个或多个主机,如下图所示,需 要指定主机地址、主机端口。

新建主机	
×	12.12.12
土 むい 思 北 ・	点分十进制整数,形如: 192.168.23.4
*主机端口:	52 (1~65535)
	确定 取消

图 9-7 新建主机页面

9.2.2 查看服务/主机

点击服务后面操作列的查看按钮⁽²⁾可以查看该服务的所有信息,点击某个主机后面的查看按钮⁽²⁾可以查看该主机的所有信息。



9.2.3 修改服务/主机

点击服务后面的修改按钮 📴 进入修改服务页面。

编辑服务				
*服务名称:	fuwu1			
*服务类型:	HTTP ¥			
*虚拟地址:	182.182.182.141			
*虚拟端口:	60	(1~65535)		
域名:				
*策略集:	无			
*记录访问日志:	◉是 ○否			
*记录防护日志:	◉是 ○否			
*负载均衡算法:	根据源IP选择			
			确定 取消	

图 9-8 反向代理模式修改服务页面

点击主机后面的修改按钮 📴 进入修改主机页面, 对主机的主机地址、主机端口进行修改。

修改主机基本信息页面如下图。

编辑主机	
×→+++114 +.L •	182.152.122
土机地址・	点分十进制整数,形如:192.168.23.4
*主机端口:	83 (1~65535)
	确定 取消



9.2.4 删除服务/主机

删除服务有两种方式:点击保护服务后面的删除按钮¹¹,将删除选择的保护服务;也可以选择一个或多个服务,点击左下方的【删除所选】进行删除。

点击保护主机后面的删除按钮 ⁶⁶,将删除选择的保护主机,当服务只剩下最后一个保护 主机时,该按钮不可用。

9.3 服务状态监控

服务状态监控界面显示当前保护服务的 HTTP/PING 响应状态信息,如下图所示。可选择



服务名称,查询各服务的状态。

服务状态监控 每页显示 20 ♥条,当前第1/1页 Ⅳ						/1页		
请选择	≩服务名称:	全部 🔽	查询					
序号	服务名称	服务	监控IP	监控端口	HTTP(S)状态	PING状态	信息	操作
1	hei	182.182.182.125:8006	182.182.182.125	8006	正常	正常	HTTP(S):HTTP/1.1 200 OK - 1491	配置 详细 更新
2	huo	182.182.182.125:801	182.182.182.125	801	正常	-	HTTP(S):HTTP/1.1 200 OK - 8289	配置 详细 更新
3	nosite	182.182.182.182:182	182.182.182.182	182	异常	-	HTTP(S):HTTP CRITICAL - Unable	配置 详细 更新

图 9-10 服务状态监控页面

站点监控界面操作列点击【配置】,可编辑站点的检测参数配置和告警配置,如下图所示:

服务状态检测				
检测参数配置				
检测内容:	□ PING			
URL域:	/			
*HOST域:	182.182.182.125:8006			
*HTTP方法域:	GET 💌			
HTTP头域:	⊙ 不指定 ○指定			
*检测间隔:	5			
告警阀值配置				
告警状态码:		】默认为空,4XX和5XX为告警状态码		
内容匹配字符串:				
*响应时间:	1.0	】默认1秒,范围为1到20		
*重复检测次数:	5	默认5次,范围为1到50		
*重复检测间隔:	1	】默认1分钟,范围为1到10		
告整配置				
* 告警状态:	● 关闭 ○ 开启			
*发送间隔:	默认5分钟,范围:1-1440			
*告警方式:	□ 邮件 □ 短信			

图 9-11 服务状态检测配置页面

检测参数配置是对检测站点状态的请求信息进行配置。告警阀值配置是配置站点状态监控 日志的相关项。其中,

▶ 检测内容, 默认使用 HTTP 方法检测, PING 和 HTTP 至少需选择一种方法;

- > 状态码, 当响应状态码不等于输入值时状态检测为异常;
- > 内容匹配字符串,当响应页面不包含输入值时响应异常;
- > 响应时间,当站点响应时间大于输入值时响应异常;
- ▶ 重复检测次数,状态异常时重复检测的次数,超过该值则不再发送异常告警;
- > 重复检测间隔,每次告警检测的时间间隔

服务状态监控界面操作列点击【详细】,可以查看站点状态正常时的响应时间图,如下图所

示。快捷查询支持最近3小时、昨天、今天、最近7天或最近30天的流量信息,也可以输入



开始时间和结束时间进行查询。

图 9-12 服务响应时间页面

第10章 漏洞扫描管理

漏洞扫描通常是指基于漏洞数据库,通过扫描等手段,对指定的远程或者本地计算机 系统的安全脆弱性进行检测,发现可利用的漏洞的一种安全检测(渗透攻击)行为。

漏洞扫描的主要功能是对 web 服务器进行扫描,以探测 web 服务器存在的安全漏洞,如 信息泄露、SQL 注入、拒绝服务、跨站脚本编制等。便于在攻击还没有发生的情况下,对 web 服务器进行安全评估,提早作出防护措施,避免黑客攻击、病毒入侵等造成的损失。

漏洞扫描管理的主界面如下图,可以实现漏洞扫描任务的新建、删除、查询、执行、停止、 删除以及扫描参数的查看。

漏洞打	編刑扫描管理 毎页显示 20 ▼条, 当前第1/1页 ↓√ [1] > 以							
-	,新建	任务名和	东:	扫描目标:		查询		
序号	选择	任务名称	任务类型	扫描目标	执行时间	当前状态	扫描报告	操作
1		test2	立即执行	182.182.182.121:86	2012-06-08 13:20:37	初始化中	查看	🏟 🚽 🔕 🖲 🛍
2		test1	立即执行	182.182.182.121:86	2012-06-06 16:51:58	扫描完成	查看	🏟 🚽 😳 🗉 🎁
全选 🗌 删除所选任务								



10.1 新建漏洞扫描任务

点击主页面的"新建"链接,进入新建漏洞扫描任务界面。如下图所示。

云枢擎天 WEB 应用防火墙用户使用手册

新建"漏洞扫描"任务			
── ● 基本配置			
*任务名称:	字母开头,字母、数字和下划线组成,长度为1到20		
*任务添加方式:	●单任务 ○批量任务		
*扫描目标:	反向代理模式下,请填写服务器真实地址。 IP:port或域名:port,端口可不填(默认为80)		
*执行方式:	●立即执行 ○将来执行 ○周期执行		
*扫描内容:	☑信息泄露 ☑ SQL注入 ☑ 操作系统命令 ☑ 跨站脚本编制 ☑ 认证不充分 ☑ 拒绝服务		
▲ 高级配置			
SSL链接:	○启用 ④不启用 用于支持扫描以HTTPS协议访问的网站		
登陆方式:	无认证 🔽		
指定URI:	◯是 ⓒ否 是否扫描指定的URI		
忽略URI:	○是 ⑧否 是否添加忽略的URI		
是否发送扫描报告:	○发送 ④不发送 是否发送扫描报告		
	确定取消		

图 10-2 新建漏洞扫描任务界面

新建任务时有基本配置和高级配置两部分,其中高级配置部分默认是隐藏的,可以通过下 展按钮显示出来或隐藏。基本配置中各个字段的解释如下:

- ▶ 任务名称:扫描任务的名字,两个漏洞扫描任务不能重名。
- 任务添加方式:有单任务和批量任务两种方式,通过单选按钮只能选择其中一种。单 任务方式每次只能添加一个漏洞扫描任务,批量任务方式每次可以添加多个漏洞扫描 任务。
- 扫描目标:扫描的网站,可以是一个 IP,也可以是一个域名,填写格式为 IP:端口, 或者域名:端口。通过选中一行信息,点击"删除选中目标"可以删除一个扫描目标。
- > 执行方式:有立即执行、将来执行和周期执行三种方式。

立即执行即在新建漏洞扫描任务成功后马上执行;

将来执行指在新建漏洞扫描任务成功后的将来的一个时间点执行,比如比当前时间晚


5 分钟执行等;

周期执行值建立的漏洞扫描任务可以周期进行扫描。

将来执行和周期执行执行时间的填写如下图所示。

*执行方式:	○立即执行	◎将来执行	○周期执行
*执行时间:	2012-06-08	15:07:07	

图 10-3 执行方式 将来执行

*执行方式:	○立即执行	○将来执行	💿 周期执行
*周期执行:	🖸 毎天 🔾 毎	周 〇毎月	
*天内时间:	15:07:07		[]]#1

图 10-4 执行方式 周期执行 (每天)

*执行方式:	○立即执行	○将来执行	⊙ 周期执行
*周期执行:	◯毎天 💽毎	周 ◯毎月	
*周内时间:	星期一 💙 1	15:07:07	

图 10-5 执行方式 周期执行 (每周)

*执行方式:	○立即执行	○将来执行	●周期执行
*周期执行:	◯毎天 ◯毎	周 💟毎月	
*月内时间:	1日 🔽 15	:07:07	

图 10-5 执行方式 周期执行 (每月)

扫描内容:包含信息泄露、SQL注入、操作系统命令、跨站脚本编制、认证不充分和 拒绝服务六项扫描内容,可以选择或取消扫描某项内容,至少选择一项。



云枢擎天 WEB 应用防火墙用户使用手册

🛋 着	5级配置	
23-0	SSL链接:	○ 启用 ③ 不启用 用于支持扫描以HTTPS协议访问的网站
	登陆方式:	认证登陆 🔽
	*用户名:	需要认证网站的用户名
	*密码:	需要认证网站的密码
	指定URI:	● 是 ○ 否 是否扫描指定的URI
	URI:	▶ 11 11 11 11 11 11 11 11 11 11 11 11 11
	*指定扫描的URI:	
		每行为一条指定扫描的URI。
	忽略URI:	○ 是 ● 否 是否添加忽略的URI
	是否发送扫描报告:	○发送 ③不发送 是否发送扫描报告

图 10-3 高级配置

SSL 链接:默认不启用 SSL 链接,扫描的是用 http 协议登陆的网站;

如果启用 SSL 链接,扫描的是 https 协议登陆的网站。

> 登陆方式:默认为无认证,扫描的网站不需要用户名密码就能访问;如果选择认证登

陆,那么需要填写登陆该网站时需要的用户名和密码,如下图所示。



图 10-5 登陆方式

指定 URL: 默认为"否",即扫描整个网站。当选择"是"单选按钮时,就会扫描指定的 URL,而不是整个网站。指定的 URL 可以逐个添加,也可以批量导入,批量导入指从本地导入一个含有多个 URL 的.txt 文件。如下图所示。

米好信 云枢擎天 WEB 应用防火墙用户使用手册 指定URI: ご是 ○否 是否扫描指定的URI URI: 添加 □ 批量导入



每行为一条指定扫描的URI。

图 10-6 指定 URI

指定URI:	●是 ○否 是否扫描指定的URI
URI:	<mark>浏览··· 导入 ☑ 批量导入</mark> 导入URI文件(.txt),每个URI为一行,形式如/bin/或/contents/1.html
*指定扫描的URI:	
	✓ 删除选中目标 每行为一条指定扫描的URI。

图 10-7 指定 URI-批量导入

- ▶ 忽略 URL: 含义和指定 URL 相反。
- > 是否发送扫描报告:默认选择不发送。如果选择发送,如图所示,则可以发送 html

或者 pdf 格式的扫描报告到指定邮箱。

是否发送扫描报告:	◎发送 ○不发送 是否发送扫描报告
*发送报告的方式:	⊙HTML ○PDF
*指定email地址:	

图 10-8 发送扫描报告



<u>
八
注意事项:</u>

指定 URL 和忽略 URL,当 URL 格式为/channels 时,代表只扫描或者只忽略 channels 这个目录;当 URL 格式为/channels/时,代表扫描和忽略 channels 这个目录 以及该目录下的所有文件。

指定 URL 和忽略 URL 中的 "是"单选按钮只能选择一个。

当选择发送漏洞扫描报告时,需要在邮件发送配置模块中配置发件信箱等信息。

首页	邮件发送配置	
系统	发信人信息	
配置	邮箱地址:	
网络配置	服务器信息	
时间配置	发送邮件服务器(SMTP):	
短信发送配置	肥久照接口(野江店の5)・	
邮件发送配置	服务部编口(款以但20)。	
HARE	登录信息	
告書配置	登录用户名:	
日志配置	登录密码:	
配置管理		旧友」モア
报表配置		休行 里亘
SMIP配置	邮件测试	
管理配置		发送测试邮件
Debug配置	测试邮箱地址:	邮件服务器配置完成后,建议你发送测试邮件,以确保配置成功。(需要网络支持)



10.2 查询漏洞扫描任务

查询条件有任务名称和扫描目标,可以根据自己的需要查询任务。如下图所示。

漏洞扫描任务显示页面还能进行每页显示条目数的调整,系统默认每页显示 20 条,还可

以显示上一页、下一页、首页和尾页。

漏洞扫描管理					毎页显示20 ✔条,当前第1/1页 🛛 √ [1] ▷ ▷
🍃 新建	任务名称:	扫描目标:	查	查询	



10.3 操作漏洞扫描任务

新建漏洞扫描任务成功后,就可以对漏洞扫描任务进行操作了。可以查看漏洞扫描报告、查看漏洞扫描详细信息、编辑漏洞扫描任务、运行漏洞扫描任务、停止漏洞扫描任务以及删除漏洞扫描任务。

对漏洞扫描任务的删除还可以通过任务下方的"删除所选任务"按钮进行删除,也可以一次全部删除所有漏洞扫描任务。

漏洞排	描管理					生	毎页显示 20 🕶	条,当前第1/1页 │○ │	[1]
	新建	任务名称	<u></u> ;;	扫描目标:		查询			
序号	选择	任务名称	任务类型	扫描目标	执行时间	当前状态	扫描报告	操作	
1		test2	立即执行	182.182.182.121:86	2012-06-08 13:20:37	扫描完成	查看	a 🖓 🖓 🎯 🗊	
2		test1	立即执行	182.182.182.121:86	2012-06-06 16:51:58	扫描完成	查看	l 🖓 🚽 😳 🗉 🛍	
全选		涂所选任务							

图 10-11 漏洞扫描任务操作列

▶ 查看扫描报告

选择一个已经完成扫描任务,点击"扫描报告"列的"查看"链接,显示出扫描任务报告, 其中有网站风险等级、扫描 IP/端口、扫描时间、任务模式、执行周期、漏洞数量等信息, 如下图所示。

任务的扫描报告	扫描时间: 2013-0	3-12 11:00:57 💌			
	H م R	·务名称:M3 陆风险等级:中介 近一次检测信息携要如	<u>ک</u> ۲:		
Filler and the	1	3描目标	扫描时间	执行时间	漏洞总计
阿贴风险等	ω Ψ λ 5	82.182.182.122:803	2013-03-12 11:00:57	1分钟	230
扫墨非大信息					
扫描基本信息	信息				
扫描基本信息 内容 任务编号	信息 1005				
扫勤基本信息 内容 任务编号 任务名称	信息 1005 ht3				
<u>お端葉本信息</u> 内容 任务儀号 任务名称 扫描IP地址端口	信息 1005 ht3 182.182.122:80	3			
扫	信息 1005 lyt3 182.182.182.122.80 2013-03-1211:00:51	3			
日勤表本信息 内容 任务编号 任务名称 日猫PH地址端口 日猫PH地址端口 月猫PH地址端口 月猫PH地址端口 月猫PH市 ()	信息 1005 ht3 182.182.182.122.80 2013-03-12 11:00.57 周期执行	3			
日勤基本信息 内容 任务编号 任务名称 日猫P地址端口 日猫P地址端口 月猫P地址端口 見描明 (1) 执行規則	信息 1005 ht3 102.182.182.122.80 2013-03-12 11:00.57 周期执行 每天 11:00:00	3			

图 10-12 扫描报告

点击屏幕右上角的导出按钮,可以将报告导出为 html 格式的文档,如下图所示。



	任务名称: M3 网站风险等级: 牛	T危 Emp.			
	扫描目标	扫描时间	执行时间	漏洞总计	
阿姑风险等级 中发	182.182.182.122:80	3 2013-03-12 11:00:57	1分钟	230	

图 10-13 导出扫描报告

▶ 查看扫描信息

选择一个扫描任务,点击"操作"列的"查看"链接,显示出扫描任务的详细信息,其中 有任务名称、扫描目标、URI 信息、登录方式、执行方式、扫描内容等。对于正在执行中 的任务,将显示当前的进度,已经完成的任务显示为100%,如下图所示。

任务名称:	lyt3
添加方式:	单任务
扫描目标:	182.182.182.122:803
是否指定URI:	不指定
是否指定忽略URI:	不指定
是否使用SSL连接:	否
登陆方式:	无需认证
执行方式:	周期执行
扫描内容:	【信息泄露】【SQL注入】【操作系统命令】【跨站脚 本编制】【认证不充分】【拒绝服务】
是否发送扫描报告:	不发送
扫描进度:	扫描已完成100%

图 10-14 查看扫描任务详细信息

▶ 编辑扫描任务

选择一个扫描任务, 点击"操作"列的"编辑"链接, 可以对扫描任务进行修改, 修改的



信息项参见"新建漏洞扫描任务"章节。

▲ 基本配置	
任务名称:	lyt3
扫描目标:	182.182.182.122:803
执行方式:	○ 立即执行 ○ 将来执行 ④ 周期执行
周期执行:	● 毎天 ○ 毎周 ○ 毎月
天内时间:	11:00:00
扫描内容:	 ☑ 信息泄露 ☑ SQL注入 ☑ 操作系统命令 ☑ 跨站脚本编制 ☑ 认证不充分 ☑ 拒绝服务
▲ 高级配置	
SSL链接:	○ 启用 ④ 不启用 用于支持扫描以HTTPS协议访问的网站
登陆方式:	无认证 💌
指定URI:	○是 ③ 否 是否扫描指定的URI
忽略URI:	○是 ● 否 是否添加忽略的URI
是否发送扫描报告:	

确定 取消



> 立刻执行扫描任务

选择一个扫描任务,点击"操作"列的"执行"链接,使该任务立刻执行。

漏洞排	調告理						毎页显示 20 💙	条,当前第1/1页 🖂 [1] 🖂
-	新建	任务名称:		扫描目标:	查询			
序号	选择	任务名称	任务类型	扫描目标	执行时间	当前状态	扫描报告	操作
1		lyt3	周期执行	182.182.182.122:803	毎天 11:00:00	扫描完成	查看	Q 🗟 💿 🛍
2		lyt2	周期执行	182.182.182.122:802	毎天 18:00:00	未执行	查看	4 / (我行) 10
з		lyt3450003	将来执行	182.182.182.122:807	2013-03-04 17:00:00	未执行	查看	C) 📝 😳 🖲 🎁
4		lyt3450002	将来执行	182.182.182.122:804	2013-03-04 17:00:00	未执行	查看	🕸 😼 😳 🗉 🎁

图 10-16 执行扫描任务

点击执行链接后,系统弹出"操作成功"对话框后,立刻执行扫描任务,如下图所示。

編洞扫描管理 每页显示 20 ♥ 条,当前第1/1页 ↓ [1]						条,当前第1/1页 🛛 🖓 [1] D 🕅			
1	新建	任务名称:		扫描目标:		查询			
序号	选择	任务名称	任务类型	扫描目标	执行时间		当前状态	扫描报告	操作
1		lyt3	周期执行	182.182.182.122:803	毎天 11:00:00		初始化中	查看	4 🕞 🗐 🗊
2		lyt2	周期执行	182.182.182.122:802	毎天 18:00:00		初始化中	查看	🎕 🛃 🔕 🖲 🛍

图 10-17 执行扫描开始执行

▶ 暂停扫描任务

对于一个正在执行中的任务,可以点击"操作列"的"停止"按钮,之后系统弹出对话框,



使当前任务停止。

漏洞打	描管理						毎页显示 20 🗸	条,当前第1/1页 🛛 🖓 [1] 🖓 🖓
3	新建	任务名称:		扫描目标:	查证	询		
序号	选择	任务名称	任务类型	扫描目标	执行时间	当前状态	扫描报告	操作
1		lyt3	周期执行	182.182.182.122:803	毎天 11:00:00	停止	查看	a 📝 🙆 🗉 🛍
2		lyt2	周期执行	182.182.182.122:802	每天 18:00:00	扫描中	查看	Q 🗟 🕲 🖬
3		lyt3450003	将来执行	182.182.182.122:807	2013-03-04 17:00:00	未执行	查看	🕸 🌛 😳 🗐 🦉

图 10-18 停止扫描任务



图 10-19 确认停止扫描任务

▶ 删除单个扫描任务

选择一个扫描任务,点击"操作"列的"删除"链接,经用户再次确认后,该任务被删除; 如果用户选择"取消",则该任务将不被删除。

	新建	任务名称:		扫描目标:	查询			
茅号	选择	任务名称	任务类型	扫描目标	执行时间	当前状态	扫描报告	操作
1		lyt3	周期执行	182.182.182.122:803	每天 11:00:00	停止	查看	4200
2		lyt2	周期执行	182.182.182.122:802	毎天 18:00:00	扫描完成	查看	🏟 🛃 🕲 🗉 🛍 🏭
3		lyt3450003	将来执行	182.182.182.122:807	2013-03-04 17:00:00	未执行	查看	🏟 🍃 🏟 🗉 🛍
4		lyt3450002	将来执行	182.182.182.122:804	2013-03-04 17:00:00	未执行	查看	🏟 📝 🏟 🖲 🛍
5		lyt3450001	将来执行	182.182.182.122:806	2013-03-04 17:00:00	未执行	查看	🏟 🛃 🎯 🗉 🛍
6		lyt6	立即执行	182.182.182.122:808	2013-03-04 16:35:00	未执行	查看	🕸 🕑 🔕 💿 🛍

10-20 删除一个扫描任务



图 10-21 确认删除

▶ 批量删除扫描任务

在扫描任务主界面中,选中多个任务行"选择"列,点击"删除所选任务",系统将删除选

中的任务,如下图所示。

漏洞打	漏洞扫描管理 每页显示 20 ℃ 条,当前第1/1页 11 √ [1] ▷▷						条,当前第1/1页 🕅 🖓 [1] 🕅	
3	新建	任务名称:		扫描目标:	查询			
序号	选择	任务名称	任务类型	扫描目标	执行时间	当前状态	扫描报告	操作
1		lyt3	周期执行	182.182.182.122:803	毎天 11:00:00	停止	查看	4 🛃 🙆 🗉 🛍
2		lyt2	周期执行	182.182.182.122:802	毎天 18:00:00	扫描完成	查看	🏟 🍺 🕲 🛍
з		lyt3450003	将来执行	182.182.182.122:807	2013-03-04 17:00:00	未执行	查看	🕸 😼 😳 🗉 🎁
4		lyt3450002	将来执行	182.182.182.122:804	2013-03-04 17:00:00	未执行	查看	🏟 🛃 🕲 🗉 🛍
5	~	lyt3450001	将来执行	182.182.182.122:806	2013-03-04 17:00:00	未执行	查看	4 😼 🙆 🗉 🛍
6	~	lyt6	立即执行	182.182.182.122:808	2013-03-04 16:35:00	未执行	查看	🕸 📝 🔕 🗉 🎁
全选	全选 曲隙所选任务							

图 10-22 批量删除任务

第11章 网页防篡改

WAF 首先从网站上将要保护的网页内容抓取下来保存到设备上,即生成本地镜像,当发生站点文件篡改后,WAF 能够很快检测到并发出告警。防篡改支持 HTTP 和 FTP 两种模式初始化,分别以不同方式防御篡改行为。当以 FTP 模式初始化后,可以启用篡改恢复功能,直接将站点上被篡改的文件恢复到原来状态。

11.1 防篡改管理

在防篡改管理页面,可以新建、编辑、删除防篡改任务,还可以查看防篡改日志,如下图 所示:

防癌改管理							
🌛 新建	ŧ						
序号	选择	名称	镜像方式	配置信息	当前状态	日志	操作
1		web	FTP	192.168.11.125:21	服务连接异常,请检查服务	查看	🏟 🛃 🛍
今· 通知266计学研究 道明: 当系统挂载设备为内存时,防箭改功能不可用							

图 11-1 防篡改管理

新建防篡改页面如下图所示:

新建防癌改服务					
*名称:	test	字母开头,字母、数字和下划线组成,长度为1到20			
*镜像方式:	FTP方式				
*IP地址:	192.168.2.88	点分十进制整数,形如: 192.168.23.4			
*端口:	21	(1~65535)			
		确定取消			



对各个字段的解释如下:

- ▶ 服务名称:防篡改任务的名字,两个防篡改任务不能重名。
- ▶ 镜像方式: FTP 两种方式

▶ IP 地址/端口:填写一个 IP 和端口,则防篡改功能对这个 IP:端口生效。

可以通过"操作"中的"编辑"按钮对当前的防篡改任务进行编辑,编辑页面同新建页面

要删除防篡改任务,可以通过"操作"中的"删除"按钮删除某一个防篡改任务,也可以通过"删除所选服务"来同时删除多个服务。

11.2 防篡改配置

需要在网站服务器端配置 FTP 服务,并把防护站点放在 FTP 服务目录下,并进行配置如

下图:

防篡改配置	
0	初始化状态:未初始化
选项	参数
服务名称:	: test
服务信息:	: 182.182.182.124:21
镜像方式:	: FTP
*目录路径:	/heike
*登录用户名:	test
*登录密码:	
	探索目录 探索完成
	该操作将探测服务ftp目录/子目录,时间依赖于目录层级以及目录数量,正常内网条件下平均0.4秒/目录

图 11-3 防篡改配置

IP 地址、端口、登录用户名、登录密码是 FTP 服务的配置,目录路径是站点在 FTP 服务 目录中的相对路径。配置好这些参数后,点击"探索目录"按钮,对站点目录进行探索。探索 的时间依赖于目录层级以及目录数量,探索完成后可看到站点下的目录,如下图所示:





服务器目录树	
□/	
🖾 /Bin/	
/SiteFiles/	
/SiteFiles/Configuration/	
/SiteFiles/Configuration/Navigation/	
/SiteFiles/Inner/	
/SiteFiles/Inner/Comment/	
/SiteFiles/Inner/Digg/	
/SiteFiles/Inner/Dynamic/	
/SiteFiles/Inner/Input/	T
添加到更新目录 添加到检测目录	
如需修改更新\检测目录列表,请勾选目录树中的目录,点击	;添加到更新\检测目录,列表将自动更新。
注: 更新目录和检测目录中添加的目录不能相互包含	
已选择更新目录	已选择检测目录
✓ /upload/	✓ /style/
☑ /中文目录显示/	

图 11-4 防篡改配置

在目录树中,可以将站点中需要更新维护的目录"添加到更新目录",将不需要更新的目录 "添加到检测目录"。需要注意的是:两个目录中不能存在相互包含的情况,比如更新目录中添 加了/SiteFiles/,则检测目录不可以再添加/SiteFiles/Configuration/。到此 FTP 方式的初始化 配置就准备好了,再点击"初始化"按钮进行网站的初始化。

初始化过程中,如果与受保护服务不能正确连接,则不能进行初始化操作。初始化所需要的时间与网络环境及防篡改配置有关。只有进行了初始化,才能进行后续的操作。

11.3 镜像同步

镜像同步操作分为两步:(1)管理员维护保护服务;(2)执行镜像同步操作。

同步镜像操作可以配置手动同步和自动同步两种方式,可以根据需要保存不同的同步方式。 同步镜像方式选择手动同步,如下图所示:



图 11-5 镜像同步-手动同步

保存配置后,点击"服务维护"后,开始站点维护。维护完成后,进行同步操作如下图所

示:

镜像同步	
0	镜像同步:服务维护中
	同步镜像方式: 💿 手动同步 🔘 自动同步 保存
	变更目录同步镜像
	 _ /flash/ _ /images/
	添加
	诸输入变更文件所在目录进行同步镜像 删除选中
	服务维护 同步镜像
	镜像同步前,诸先进行服务维护,再进行同步镜像

图 11-6 镜像同步-服务维护

在变更目录中,添加站点在维护过程中修改过的文件或网页所在的目录。注意这里应当是初始化配置中更新目录或检测目录的子集。添加完毕后,选择"同步镜像"。

同步镜像方式选择自动同步时,界面如下所示:

镜像同步	
0	镜像同步:成功 最近一次执行时间:2012-07-09 22:37:50
	同步镜像方式: 🔿 手动同步 💽 自动同步 保存
	服务器维护时间: 09:00
	同步镜像时间: 10:00

设定服务器维护时间和同步镜像时间,保存配置,则开启了自动同步镜像功能。防篡改会 从服务器维护时间开始后暂停,在到达同步镜像时间后,设备会自动将在这个时间段修改的站 点内容同步到镜像文件。

同步镜像操作有相应的日志,可以根据日期进行查询,也可根据"详细"链接查看此次镜 像内容变化的详情。

11.4 篡改检测

篡改检测页面如下图所示,可以设置篡改检测的开启和关闭,可以设置篡改检测间隔。篡 改检测日志可以在防篡改日志中查询到。

篡改检测				
0	篡改检测状态:开启			
	篡 改检测:	开启	关闭	
	篡改检测间隔 :	5	秒	保存
	图 11	-8 篡改校	金测	

图 11-7 镜像同步-自动同步

第12章 **日志**

日志模块用于记录和显示系统各功能模块的运行历史,主要包括系统日志、服务访问日志、 认证日志、服务监控日志、告警日志、web 防护日志、漏洞扫描日志、防篡改日志、漏洞扫描 日志。

12.1 系统日志

主要记录与 WAF 配置相关的日志,如下图所示,显示的信息有:

- ▶ 时间:日志生成的时间,具体到秒。
- > 登录 IP:操作 WAF,使生成系统日志的源 IP。
- ▶ 用户:显示用哪个用户在操作 WAF。
- ▶ 事件:显示操作的是哪个模块。
- ▶ 摘要:简要的描述日志。
- ▶ 日志级别:显示系统日志的级别。
- > 状态:用户的操作是否成功,若没有配置成功,则显示"失败"。

+		时间	── 范围 ⁹ E	Start: 2013-03-19	00:00:00 AND AND AND			
+] 🖸	选择搜索条件	👻 😽 💌		查询			
N	e Pa	选择搜索条件 9 ⁸ 登录旧						Displaying 1 - 40 of 377
	时间	用户	用户	亊件	摘要	日志级别	状态	
1	2013		admin	服务管理	编辑服务,名称为:tt	信息	成功	<u>^</u>
2	2013	03日志级别	admin	服务管理	新建服务,名称为:tt	信息	成功	
з	2013	□状态 03-19-16:42:50 192-168-2	uus admin	服务管理	编辑服务,名称为:web803	信息	成功	

图 12-1 系统日志

系统日志查询,用户可以自己定义搜索条件,例如登录 IP、用户、时间、摘要、日志级别、 状态,可以与系统默认的查询条件"时间"进行"与/或"组合查询搜索。 如果有大量的系统日志,用户还可以通过页面跳转(上页、下页、首页、尾页)。

12.2 访问日志

12.2.1 服务访问日志

访问日志记录了客户端访问 WAF 保护的服务的记录。如下图所示,默认显示的信息有时间、客户端地址、地址来源、服务名称、访问 URL、服务 IP:PORT、方法、HTTP 状态、响应时间等。此外,还可以通过每个字段右边的下拉箭头选择排序方式升序或者降序。

▶ 首页	服务订	方问日志						默认查询当	运行,如需	查看历史日志请选	择条件查询
 系统 				Chart 2	013-03-19 00:0	0:00					
・ 配置	+		🖌 🤨	BV Start.	2013-03-19 17 ⁻ 0	3:37 直	询				
▶ 策略				End :		Jun					
▶ 服务	19	Page 1 of 15016	7 ▶ ▶ 💞							Displaying 1 - 40	of 6006678
 对象库 		时间	客户端地址	地址来源	服务名称	访问URL	服务IP:Port	方法	HTTP状态	响应时间	
▶ 检测		2013-03-19 17:03:06	182.182.182.115	巴基斯坦	web803	/cat.php?cid=14	182.182.182.123:803	GET	502	2	^
• 防护	- 2	2 2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p_heike	/SiteFiles/Inner	182.182.182.125:8006	POST	403	0.000	
、法备代化	3	2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p_heike	/images/about	182.182.182.125:8006	GET	304	0.003	
· ULEVER	1	2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p_heike	/images/3pxl.gif	182.182.182.125:8006	GET	404	0.000	
▶ 防病毒		5 2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p_heike	/images/dsf.jpg	182.182.182.125:8006	GET	304	0.004	
▶ 集成认证	6	2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p_heike	/images/about	182.182.182.125:8006	GET	304	0.000	
▼ 日志	3	2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p_heike	/images/home	182.182.182.125:8006	GET	304	0.000	
系统日志	6	2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p_heike	/images/menu	182.182.182.125:8006	GET	304	0.000	
访问日志 🝷	9	2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p_heike	/images/menu	182.182.182.125:8006	GET	304	0.001	
服务访问日志	16	2013-03-19 17:03:06	182.182.182.115	巴基斯坦	p heike	/imades/menu	182.182.182.125:8006	GET	304	0.000	

图 12-2 服务访问日志

· 首页	服务订	方问日志						
系统	+	- 时间	.	范围▼				
配置	Star	t: 2017-01-09 00:00	:00	XSLB				
▶ 对象库	End	: 2017-01-09 15:58	3:42					
▶ 缺省规则	AND							
▶ 策略	+	- 选择搜索条件	•	等于 ▼		AND		
▶服务	+	客户端地址		→ ▼		查询		
▶漏扫		Pa 服务名称 访问URL	_					
▶ 防算改		时间 服务IP:Port		地址来源	服务名称	访问URL	服务IP:Port	方法
D±	1	2016 万法		局域网	web	/demo/search	192.168.11.103:8001	GET
· 山心	2	2016-12-28 10:20:33	192.168.11.1.	局域网	web	/demo/1989.f	192.168.11.103:8001	GET
系统日志	3	2016-12-28 10:20:33	192.168.11.1	局域网	web	/demo/1989.f	192.168.11.103:8001	GET
切回日志 🔹	4	2016-12-28 10:20:23	192.168.11.1.	局域网	web	/favicon.ico	192.168.11.103:8001	GET
服务功回日志	5	2016-12-28 10:20:21	192.168.11.1	局域网	web	/demo/1989.f	192.168.11.103:8001	GET
事件口志 防拍日主	6	2016-12-28 10:20:21	192.168.11.1	局域网	web	/demo/attach	192.168.11.103:8001	GET
おお	7	2016-12-28 10:20:21	192.168.11.1	局域网	web	/demo/1989.f	192.168.11.103:8001	GET
1040	8	2016-12-28 10:20:21	192.168.11.1	局域网	web	/demo/1989.f	192.168.11.103:8001	GET
	9	2016-12-28 10:20:21	192.168.11.1.	局域网	web	/demo/1989.f	192.168.11.103:8001	GET
	10	2016-12-28 10:20:21	192.168.11.1	局域网	web	/demo/1989.f	192.168.11.103:8001	GET

图 12-3 服务访问日志-查询条件

服务访问日志查询,用户可以自己定义搜索条件,在下拉框中选择服务名称、客户端地址、方 法、URL 地址、服务 IP:Port,可以与系统默认的查询条件"时间"进行"与/或"组合查询

搜索。

如果有大量的系统日志,用户还可以通过页面跳转(上页、下页、首页、尾页)。

12.3 事件日志

事件日志有一种,告警日志。告警日志记录告警,告警配置需要在配置模块中操作。

12.3.1 告警日志

要生成告警日志,必须首先在告警模块进行配置,如图所示,可以配置 WEB 攻击告警、 网页篡改告警、设备状态告警、服务状态告警、漏洞扫描告警、HA 配置告警。

WEB攻击告警 阿尔	页篡改告警	设备状态告警	服务状态告警	漏洞扫描告警	HA配置告警	
告警管理-漏洞扫描						
	告警开关:		◉ 开启 ◎关闭]		提示: 告警在每个扫描任务执行完毕后进行
	告警方式:		🕑 邮件 🔲 短信	Ì		
	接收邮箱:		meng1103@1	26.com	li	邮件之间用半角的逗号(即英文的逗号)分隔; 仅允许输入10个Email。
						保存重置

图 12-4 告警配置

告警日志可以查看时间、服务名称、主机地址、类型、状态、信息、邮件、邮件发送结

果、手机、短信发送结果等信息。支持分页功能。如图所示。

• 首页	皆警日志 默认查询当天日志,如需查看历史日志请选择条件	查询
• 系统	Chart - 2013-03-19 00:00 00 📷	
• 配置	+ 时间 v 范围 v 2013 03 19 17 09:45 重询	
 策略 	End : 20130010 17.00.45	
▶ 服务	4 4 Page 1 of 1 > > 20 Displaying 1 - 18 d	of 18
 对象库 	时间 服务名称 -> 主机地址 类型 状态 信息 邮件 邮件关送结果 短信 短信发送结果	
• 检测	1 2013-03-18 15:53:50 xie_heike 182.182.1 服务状态 警告 182.182.1 xiezmb 未成功 18601292122 未成功	^
· Eta	2 2013-03-18 15:21:10 huoxian - 网页篡改 警告 篡改检测: caoyia 成功 未发送	
* #J#	3 2013-03-18 15:50:20 cao_linux 182.182.1 服务状态 警告 CRITICAL xiezmb 未成功 18601292122 未成功	
• 派皇兀化	4 2013-03-19 10:42:46 漏洞扫描 警告 任务ID:10xiezmb成功 18601292225 未成功	
▶ 防病毒	5 2013-03-19 10:46:39 漏測3描 警告 任务ID:10 xiezmb 成功 18601292225 未成功	
▶ 集成认证	6 2013-03-19 10:47:30 潇澜扫描 警告 任务D:10,成功 1860129225 未成功	
▼ 日志	7 2013-03-19 10:48:21 漏洞扫描 警告 任务ID:10xiezmb成功 18601292225 未成功	
系统日志	8 2013-03-19 10:49:24 漏洞扫描 警告 任务ID:10xiezmb成功 18601292225 未成功	
访问日志	9 2013-03-19 10:50:25 漏洞扫描 警告 任冬[D:10xiezmb成功 18601292225 未成功	
事件日志 ▼	10 2013-03-19 10:56:34	
服务监控日志	11 2013-03-19 13:28:01 漏洞扫描 警告 任务ID:10 xiezmb 成功 18601292225 未成功	
HSHE	40.0110.01.01.010.01.00	

图 12-5 告警日志

告警日志查询,用户可以自己定义搜索条件,在下拉框中选择服务名称、主机地址、类型、 状态、信息,可以与系统默认的查询条件"时间"进行"与/或"组合查询搜索。



云枢擎天 WEB 应用防火墙用户使用手册

告警日	志								默认查询当天日	日志,如需查看历史日末	总请选择条件查询
+) 💽	时间	💌 范围 💌	Start: 20 End : 20	13-03-19 13-03-19	00:00:00 17:08:45					
+) 🖸	选择搜索条件 选择搜索条件	(学生)	~		查询	ו				
14 8	Pag	* 服务名称								Disp	laying 1 - 18 of 18
	时间	主机地址	ŧ L ‡也址	类型	状态	信息	邮件	邮件发送结果	短信	短信发送结果	
1	2013-0	- 突型 - 状态	2.182.1	服务状态	警告	182.182.1	xiezmb	未成功	18601292122	未成功	^
2	2013-0	信息		网页篡改	警告	篡改检测:	caoyja	成功		未发送	

图 12-6 告警日志查询

如果有大量的告警日志,用户还可以通过页面跳转(上页、下页、首页、尾页)。

12.4 防护日志

防护日志有三种:防篡改日志、漏洞扫描日志、WEB 防护日志。

12.4.1 防篡改日志

显示防篡改日志信息。如图所示,防篡改日志可以显示开始时间、结束时间、服务名称、 服务信息、镜像方式、执行任务、添加文件数、删除文件数、篡改文件数等信息。点击"详细" 列"查看"按钮,可以查看详细信息。

・ 配置	A	自改摘要日志							默认查询	当天日志,如常	<u>-</u> 査着历史	日志请选择条件查询
 策略 					2013-03-19-00-00-0	0 000						
▶ 服务		+ 开始时间	🖌 范	🗉 🗹 Start	2012 02 10 00:00:0	1	查询					
▶ 对象库				End	: 2013-03-13 17.12.2							
▶ 检测	14	4 Page 1 of 25									C	isplaying 1 - 40 of 961
▶ 防护		开始时间	结束时间	服务名称	服务信息	镜像方式	执行任务	添加文件数	删除文件数	篡改文件数	详细	
、流量优化		1 2013-03-19 17:11:50	2013-03-19 17:11:51	new	182.182.182.115:21	FTP	篡改检测	0	0	0	查看	^
, 阶座车		2 2013-03-19 17:10:50	2013-03-19 17:10:50	new	182.182.182.115:21	L FTP	篡改检测	0	0	0	查看	
• 购物器		3 2013-03-19 17:09:49	2013-03-19 17:09:50	new	182.182.182.115:21	FTP	篡改检测	0	0	0	查看	
▶ 集成认证		4 2013-03-19 17:08:49	2013-03-19 17:08:49	new	182.182.182.115:21	FTP	篡改检测	0	0	0	查看	
▼ 日志		5 2013-03-19 17:07:48	2013-03-19 17:07:48	new	182.182.182.115:21	FTP	篡改检测	0	0	0	查看	
系统日志		6 2013-03-19 17:06:47	2013-03-19 17:06:48	new	182.182.182.115:21	FTP	篡改检测	0	0	0	查看	
访问日志		7 2013-03-19 17:05:46	2013-03-19 17:05:47	new	182 182 182 115:21	ETP	篡改检测	0	0	0	查看	
事件日志		o 2013-03-10 17:04:46	2013-03-10 17:04:46	new	182 182 182 115:21	FTD	第改检测	0	0	0	杳若	
防护日志 🔻		8 2010-00-19 17:04:40	2010-00-19 17:04:40	11044	102.102.102.115.21		20120720-301	0	0	0	本系	-
TEB防护日志		9 2013-03-19 17:03:45	2013-03-19 17:03:45	new	182.182.182.115:21	L FIP	大学に大学生(例)	U	2	0	三個 十 五	
防算改日志	1	10 2013-03-19 17:02:45	2013-03-19 17:02:45	new	182.182.182.115:21	L FTP	暴吹碰測	0	0	0	宣看	

图 12-7 防篡改日志

防篡改日志查询,用户可以自己定义搜索条件,在下拉框中选择服务名称、服务信息、镜像 方式、执行任务、添加文件数、删除文件数、篡改文件数,与系统默认的查询条件"时间"进行"与/或"组合查询搜索。



云枢擎天 WEB 应用防火墙用户使用手册

防篡改	<u> (摘要日</u>)	志							默认查询	当天日志,如需	渣看历史	日志请选择条件查试
+		开始时间	🖌 🤨	Start End	2013-03-19 00:00:00		AND					
+) 🖸	选择搜索条件 选择搜索条件	💉 😽	- 🖌		查询						
14	4 Pag	服务名称									C	isplaying 1 - 40 of 96
	开始时间	服务信息		服务名称	服务信息	镜像方式	执行任务	添加文件数	删除文件数	篡改文件数	详细	
1	2013-0	現像方式 执行任务	:51	new	182.182.182.115:21	FTP	篡改检测	0	0	0	查看	
2	2013-0	添加文件数	0:50	new	182.182.182.115:21	FTP	篡改检测	0	0	0	查看	
З	2013-0	」 「開床又1+致 篡改文件数	9:50	new	182.182.182.115:21	FTP	篡改检测	0	0	0	查看	

图 12-8 防篡改日志查询

如果有大量的防篡改日志,用户还可以通过页面跳转(上页、下页、首页、尾页)。

12.4.2 漏洞扫描日志

记录漏洞扫描的结果并可以查看详细结果。如图所示,可以显示任务名称、扫描目标、执行时间和漏洞数目信息,支持分页功能。点击"操作列"的详细链接,则可以查看漏洞扫描报

Æ	
	0

RT ^	漏港	扫描日志						默认查询当天日志,如需查看历史日志诸选择条件查询
策略				201	3-03-19-00-00-	00		
服务		执行	时间 🔽	范围 🖌 Start:	3.03.19 17:14	05 查询		
对象库				End : 201	5.05.10 11.14			
检测	14	4 Page 1	of 1 🕨 🕅 🍣					Displaying 1 - 21 of 21
防护		任务名称	扫描目标	执行时间	漏洞数目	扫描时间(分钟)	操作	
流量优化		1 lyt5	152.152.152.122:808	2013-03-19 14:09:39	7	1	详细	<u>^</u>
<u>於定</u> 其		2 lyt5	152.152.152.122:808	2013-03-19 13:44:50	7	1	详细	
(0) 70 60 (在 cP>1) 7		3 lyt5	152.152.152.122:808	2013-03-19 13:30:01	7	1	详细	
<u> </u>		4 lyt1	152.152.152.122:802	2013-03-19 13:26:45	34	1	详细	
日志		5 lyt5	152.152.152.122:808	2013-03-19 10:48:25	7	1	详细	
系统日志		5 lyt4	152.152.152.122:807	2013-03-19 10:47:24	7	1	详细	
访问日志		7 lyt3	152.152.152.122:806	2013-03-19 10:46:23	7	1	详细	
爭件日志 除於日本		B lyt2340003	152.152.152.122:804	2013-03-19 10:45:22	3408	11	详细	
助ず口志 ▼		9 lyt2340002	152.152.152.122:803	2013-03-19 10:45:21	230	4	详细	
1120回デロ忌 防省改日士	1	0 lyt2340001	152.152.152.122:802	2013-03-19 10:45:19	34	1	详细	
漏洞扫描日志	1	1 lyt1	152.152.152.122:802	2013-03-19 10:41:20	34	1	详细	

图 12-9 漏洞扫描日志

漏洞扫描日志查询,用户可以自己定义搜索条件,在下拉框中选择任务名称、目标 IP、目标动动力,漏洞数目和扫描时间进行查询,与系统默认的查询条件"时间"进行"与/或"组合

查询搜索。

漏洞扫	描日志						默认查询当天日志,如需查看历史日志请选择条件查询
+		执行时间	○ 范围 ▼ Start: 2013 End : 201	3-03-19 00:00:00 3-03-19 17:14:06			
+		选择搜索条件	等于 🖌		查询		
14 4	Pag	选择搜索条件 [●] 任务名称					Displaying 1 - 21 of 21
	任务名	彩目标IP	执行时间	漏洞数目	扫描时间(分钟)	操作	
1	lyt5	日155% 日	2013-03-19 14:09:39	7	1	<u>详细</u>	<u>^</u>
2	lyt5	扫描时间	2013-03-19 13:44:50	7	1	详细	

图 12-4 防篡改日志查询

如果有大量的漏洞扫描日志,用户还可以通过页面跳转(上页、下页、首页、尾页)。

12.4.3 WEB 防护日志

WEB 防护日志用于所有 web 防护类型的日志信息。

如图所示, WEB 防护日志可以显示时间、服务名称、策略名称、源地址、方法、URL 地址、攻击分类、详细类型、防护状态、HTTP 状态、匹配值等信息。支持分页功能。

▶ 配置		WEBR	访护日志							默认	查询当天日	志,如需查着	历史日志	清选择条	件查询
▶ 策略	-					ourse, 2013-03	3-19 00:	00:00							
▶ 服务		+) 🕞 时间		▼ 范围 ▼	5tart - 2013-01	B-19 17	10:58	查询						
▶ 对象库						End : Lorook		10.00							
▶ 检测		14	Page 1 of 1064	183 🕨 🕅	12								isplaying 1	- 40 of 42	59314
▶ 防护			时间	服务名称	策略名称	源地址	方法	URL地址	攻击分类	详细类型	防护动作	HTTP状态	匹配值	操作	
→ 流量优化		1	2013-03-19 17:10:42	web803	P-lifang4	182.182.182.1	GET	/scanner.asp	爬虫防护	Robots/deny	阻止	502	eCatch		^
防病毒		2	2013-03-19 17:10:42	web803	P-lifang4	182.182.182.1	GET	/listen.aspx?s	爬虫防护	Robots/deny	阻止	502	geck		
生成认证		3	2013-03-19 17:10:42	web803	P-lifang4	182.182.182.1	GET	/blur.shtml?s	爬虫防护	Robots/deny	阻止	404	geck		
		4	2013-03-19 17:10:42	web803	P-lifang4	182.182.182.1	GET	/beatles?gro	爬虫防护	Robots/deny	阻止	404	china		
• 日志		5	2013-03-19 17:10:42	web803	P-lifang4	182.182.182.1	GET	/robot.shtml	爬虫防护	Robots/deny	阻止	404	sitesn		
系统日志		6	2013-03-19 17:10:42	web803	P-lifang4	182.182.182.1	GET	/robot.jsp?us	爬虫防护	Robots/deny	阻止	404	fastlw		
访问日志		7	2013-03-19 17:10:42	web803	P-lifano4	182,182,182,1	GET	/hello.htm?p	基本攻击防护	BasicAttack/	阻止	404	/hello		
事件日志			2013-03-19 17-10-42	web803	P-lifano4	182 182 182 1	GET	/blur.btm2ar	爬电防护	Robots/denv	阳止	404	nchro		
防护日志 188防护日志	-	9	2013-03-19 17:10:42	web803	P-lifang4	182.182.182.1	GET	/listen.html?	爬虫防护	Robots/deny	阻止	404	mosia		

图 12-5 WEB 防护日志

WEB防护	旧志							每页显示 20 ▼	条,当前第1/1页 🖂 [1] 🖂
规则分类:	全部	▼ 规则ID:		攻击地址:					
开始时间:	2017-01-09 00:00:00	🔄 💷 结束时间:	2017-01-09 16:01:06		查询				
序号	时间		规则ID	事件	动作	规则集	攻击分类	攻击地址	服务
1	2016-12-28 10:20:51		959071	详细	禁用	缺省规则	SQL 注入攻击	192.168.11.130	web
2	2016-12-27 20:12:24		959071	详细	禁用	缺省规则	SQL 注入攻击	192.168.11.19	web

图 12-6 WEB 防护日志查询

告警日志查询,用户可以自己定义搜索条件,按照规则分类、规则 id、攻击地址、攻击时间

进行组合查询搜索。

如果有大量的 web 防护日志,用户还可以通过页面跳转(上页、下页、首页、尾页)。



第13章 **报表**

报表模块包含时段综合统计、服务综合统计、WEB 攻击统计报表统计。这些报表不同角度 分析防护网站的被访问情况,统计各种类型攻击,更直观、深入的展现了防护网站的运行及安 全状态,为网站管理和防御提供了更好的依据。

13.1 时段综合统计

时段综合统计报表主要针对 WEB 攻击防护。

时段分析有日段分析、周段分析和月段分析三种。各个部分的日段分析、周段分析、月段 分析图总坐标都是攻击次数或者访问次数,横坐标不同,日段分析以以小时为单位显示一天 24 小时内的攻击或者流量情况,周段分析以一周内的自然天为单位显示一周内的攻击或者流量情况,月段分析以一月内的自然天为单位显示一月内的攻击或者流量情况。

登录成功后点击左侧导航"报表管理"-"时段综合统计"项,进入此界面。



图 13-1 时段综合统计报表

▶ 服务名称

进入"时段综合统计"界面,"服务名称"系统默认为"全部",点击下拉菜单,可以选择

需要统计的某个服务,或者选择"全部",如下图所示。

▶ 时段分析

进入"时段综合统计"界面,"时段分析"系统默认为"日段分析",点击下拉菜单,可以选择需要统计的时间段,"日段分析""周段分析""月段分析",如下图所示。

的技际合统的	+报表							12
服务名称:	全部 ✓ 全部	时段分析:	月段分析 💙	统计时间:	2013-03		查询	
▲ WEB攻击的	lyt1(182.182.182. lyt2(182.182.182.1 lyt3(182.182.182.1 ow_1haodian(112							
时段综合统	计报表							
时段综合统 服务名称:	计报表	时段分析:	月段分析 💌 日段分析	统计时间:	2013-03	111	查询	1

图 13-5 服务名称与时段分析设置

▶ 统计时间

进入"时段综合统计"界面,"统计时间"系统默认为当前日期,从0点开始到当前时间, 点击下拉菜单,可以选择开始统计的时间。

▶ 统计导出

进入"时段综合统计"界面,点击屏幕右上角的图标,可以将报表导出为 html 格式文档, 如下图所示。

时段综合统	计报表						
服务名称:	全部	*	时段分析: 月段分析 🛩	统计时间:	2013-03	查询	导出为HTML



13.2 服务综合统计

访问是对某个保护服务的被攻击网站进行分析统计。包括从访客 IP、访问来源、最常访问



云枢擎天 WEB 应用防火墙用户使用手册

网页、入站出站、找不到的网页、站点域名等角度统计,如下图。TOP 可以选择前 10、20、

50或100。

※ 米好信安				admin 2 您好,您当被角色是:都回管理员。
• 首页	服务综合统计报告			3
 ・私境 ・ 配置 	服务名称: 全部 •	续计时间: 2014-12-23 00:00:00 📄 到 2014-12-23 12:58:39 📄		意识
 対象库 ・ お客様別 	ム 法间接计 当前服务:全部			
 第 	分点点型: [5/茶IP ・ TOP 10 ・			四未失型: (14)四 •
 ・服务 ・ ・ ぶ白 ・ 			0.00	Bulletone B
• 附算改	1944 19 東田市道 19回2100日里 警売鉄橋	阿尔切肖里克多	辛田県	\$212 VSI 4941 MB
 日志 - 报表 				
时投标合统计				
服务综合设计 Web攻击统计				

图 13-7 服务综合统计

	い 当時服务・主	a9	
分类类型:	访客IP 🔽	TOP 10 💌	图表类型: 饼状图 💌
	访客IP 访问来源 最常访问的网页 入站出站 找不到的网页 站点域名		

图 13-8 访问统计-分类



图 13-9 访问统计-访问来源





图 13-10 访问统计-入站出站

点击右上角"导出 HTML 格式报表"的图标 4. 系统弹出对话框如下,系统默认文件

名为 html.tar 文件,选择文件的本地存储位置。

	另存为
或保存此文件吗? 名称: htal.twr 类型:300压绳:54000 从: 182.182.182.131 打开 ① 保存 ⑤) 取消 成文件和記名是嘲问 ② 相目 Taiteration 的文件實驗的沒有所帮助,但至些文件可能 爱您的计准和,如果您不信任其采撷,请不要打开或保存 变文件,直復回驗?	 保存在 Q): 資 魚面 ③ 分 P 四・ ③ 分 P 四・ ③ 分 P 四・ ○ 分 P 回 の P
	文件名(1): 1011100 (現在) (1): 1011100 (現在) (1): 1011100 (現在) (1): 10111000 (1): 10111000 (1): 10111000 (1): 10111000 (1): 10111000 (1): 10111000 (1): 10111000 (1): 101100000000000000000000000000000000

图 13-11 导出 HTML 格式报表

在本地磁盘存储后,对此文件进行解压,双击 WAF_report.html 文件,即可显示统计报表的内容。



图 13-12 打开导出的 HTML 报表

注意:如果浏览器限制此网页运行可以访问计算机的脚本或 Active 控件,请点击"允许阻止的内容"选项,以便此报表的正确显示。

13.3 WEB 攻击统计

WEB 攻击统计报表包括被攻击目标的分布、按攻击类型统计、按攻击源地址统计、按攻击

云枢擎天 WEB 应用防火墙用户使用手册

来源统计、按访问方法统计、受攻击最多的 URLTOP 排名六部分,每部分以服务划分,用户需选择服务和统计时间段。

登录成功后,点击左侧导航"报表"-"web 攻击统计"项,进入 WEB 攻击统计报表主界面,可以导出为 HTML 格式报表到本地磁盘。点击屏幕右上角的"导出 HTML"按钮,可以将报表导出到本地,经解压后可以打开查看报表。

ġ.		14				admin 📿 😥	F,愈当前角色是:超级管理
Web攻击统计报表							2
服务名称: 全部	•	统计时间	2014-12-23	2014-12-23			应用
← 被攻击目标的分布	当前服务:全部						
							間表意想: 柱状間 *
			新生活的				
2年	服务名称		870034	主机的社		攻击次数	新古爾分比
暂无趋据							
△ 接攻击类型统计	当前服务: 全部						
救援要示 Top10	٠						四大共型: 柱状因 *
			暂无该图				
暂无约据	尾萼	攻击突型		攻击灭胜		双击犯事	
← 技攻击激地址统计	当前服务:全部						
數據豐示 Top10	٠						四天类型: 柱状四 *
			暂光波图				
	序号	攻击運10	地址	攻击次数		占总攻击次数的面分比	
暂无此据							
▲ 按访问方法统计	当前服务:全部						
							四赤典型: 住状団 ・
			替无谈团				
新王作用	序号		访问方法		攻击次政	占范攻击次最的百分比	
A 50484000	TOP請在 内前服表: 企業						
数据22元 10p10	•						四新常型: [1103] *

图 13-13 WEB 攻击防护报表

13.3.1 被攻击目标的分布

统计被攻击的目标。可以显示柱状图、饼状图和折线图。图例中,横坐标中是多个被攻击



的目标,纵坐标是被攻击的次数。

图 13-14 被攻击目标的分布

13.3.2 按攻击类型统计

统计攻击类型。可以显示柱状图、饼状图和折线图。图例中, 横坐标中是多个被攻击的类

型,纵坐标是该类型攻击的次数。



图 13-15 按攻击类型统计

13.3.3 按攻击源地址统计

统计攻击源地址。可以显示柱状图、饼状图和折线图。横坐标中是多个发起攻击的源地址,



纵坐标是该地址攻击的次数。





13.3.4 按访问方法统计

统计访问方法。可以显示柱状图、饼状图和折线图。图例中,横坐标中是攻击方法,访问

方法有 GET、POST 和其他三种方式,纵坐标是该类型攻击的次数。





13.3.5 受攻击最多的 URLTOP 排名

统计受攻击最多的 URL。可以显示柱状图、饼状图和折线图。



图 13-18 受攻击最多的 URL 统计



附录

1. 出厂配置

1.1通讯口初始配置

図ロ	IP
带外口	https://192.168.45.1

1.2Web 用户初始配置

用户名	admin
密码	admin123

1.3命令行用户初始配置

用户名	root
密码	esv0812



1.4管理口

产品型号	管理口
WAF 6 接口	eth5
WAF 11 接	eth10
П	

1.5串口

串口	console
波特率	19200

2. WAF 在多链路环境下的路由配置

2.1 WAF 中的路由介绍

WAF 作为网关产品需要适应不同的网络环境,特别是透明模式下,环境比较复杂。此时为了保证服务的可访问、可防护和状态可监控,保证漏洞扫描、防篡改等功能可用,需要进行相关的路由配置。配置方法如下:

1, 为没有 IP 的链路, 增加如下静态路由:

链路 IP 所在网段/网段掩码/0.0.0./链路接口 (不包括 br_default 桥)

2, 若多个链路在同一网段, 则需为多个链路上的每个服务增加如下静态路由:

服务 IP/255.255.255.255/0.0.0.0/链路接口

3,为每个链路,增加如下策略路由:

0.0.0.0/0.0.0./链路网段网关/链路接口 (不包括 br_default 桥)

服务 IP/255.255.255.255/0.0.0.0/链路接口 (不包括绑定到 br_defautl 桥的服务)

2.2 配置示例

注:

- 1, 如下示例中链路不仅包含普通桥, 也包含 VLAN 链路, 没有进行区分说明。
- 2, br_default 桥默认有 IP, 不再单独说明。
- Trunk 链路与普通链路类似,区别仅在于多个链路使用同一对物理端口,每个 VLAN 链路由该对物理端口的对应的虚拟子接口组成。
- 4, 蓝色字体的配置的是为了保证服务状态监控、漏洞扫描等功能的正常使用, 这些功能 需要链路配置 IP。

2.2.1 多链路不在同一网段且每链路上都有 IP

路由配置:

1, 只需为每个链路各增加策略路由即可:

0.0.0.0/0.0.0./链路网段网关/链路接口(不包括 br_default 桥)

服务 IP/255.255.255.255/0.0.0.0/链路接口 (不包括绑定到 br_defautl 桥的服务)

示例:

拓扑:





F-1多链路不在同一网段且每链路上都有 IP

配置:

0.0.0.0/0.0.0.0/192.168.1.254/br_test1/策略路由

0.0.0.0/0.0.0.0/192.168.2.254/br_test2/策略路由

192.168.1.50/255.255.255.255/0.0.0.0/br_test1/策略路由

192.168.2.50/255.255.255.255/0.0.0.0/br_test2/策略路由

2.2.2 多链路不在同一网段且链路上没有 IP

路由配置:

1, 为每个链路增加1条静态路由

链路 IP 所在网段/网段掩码/0.0.0./链路接口 (不包括 br_default 桥)

2, 为每个链路增加1条策略路由

0.0.0.0/0.0.0./链路网段网关/链路接口(不包括 br_default 桥)



示例:

拓扑:



图 F-2 多链路不在同一网段且链路上没有 IP

配置:

192.168.1.0/255.255.255.0/br_test1/静态路由

192.168.2.0/255.255.255.0/br test2/静态路由

0.0.0.0/0.0.0.0/192.168.1.254/br_test1/策略路由

0.0.0.0/0.0.0.0/192.168.2.254/br_test2/策略路由

2.2.3 多链路在同一网段且每链路上都有 IP

路由配置:

1, 为每个服务增加1条直连路由

服务 IP/255.255.255.255/0.0.0.0/链路接口

2, 为每个链路增加策略路由



0.0.0.0/0.0.0./链路网段网关/链路接口 (不包括 br_default 桥)

服务 IP/255.255.255.255/0.0.0.0/链路接口 (不包括绑定到 br_defautl 桥的服务)

示例:

拓扑:



图 F-3 多链路在同一网段且每链路上都有 IP

配置:

192.168.0.50/255.255.255.255/0.0.0.0/br_default/静态路由

192.168.0.51/255.255.255.255/0.0.0.0/br_test1/静态路由

192.168.0.52/255.255.255.255/0.0.0.0/br_test2/静态路由

0.0.0.0/0.0.0.0/192.168.0.254/br_test1/策略路由

0.0.0.0/0.0.0.0/192.168.0.254/br_test2/策略路由

192.168.0.51/255.255.255.255/0.0.0.0/br_test1/策略路由

192.168.0.52/255.255.255.255/0.0.0.0/br_test2/策略路由



2.2.4 多链路在同一网段且链路上没有 IP

路由配置:

1, 为每个服务增加1条直连路由

服务 IP/255.255.255.255/0.0.0.0/链路接口

2, 为每个链路增加1条主路由

链路 IP 所在网段/网段掩码/0.0.0./链路接口 (不包括 br_default 桥)

3, 为每个链路增加策略路由

0.0.0.0/0.0.0./链路网段网关/链路接口 (不包括 br_default 桥)

示例:

拓扑:



图 F-4 多链路在同一网段且链路上没有 IP

配置:

192.168.0.50/255.255.255.255/0.0.0.0/br_default/静态路由

192.168.0.51/255.255.255.255/0.0.0.0/br_test1/静态路由



192.168.0.52/255.255.255.255/0.0.0.0/br_test2/静态路由

192.168.0.0/255.255.255.0/br_test1/静态路由

192.168.0.0/255.255.255.0/br_test2/静态路由

0.0.0.0/0.0.0.0/192.168.0.254/br_test1/策略路由

0.0.0.0/0.0.0.0/192.168.0.254/br_test2/策略路由

2.2.5 综合情况

若 WAF 中的多链路即有在同一网段,也有不在同一网段的,即有带 IP,也有没有 IP,此 时的路由配置需要进行按照步骤逐一分解配置即可。

示例:

拓扑:
云枢擎天 WEB 应用防火墙用户使用手册





图 F-5 综合情况

拓扑说明:

- br_default 和 v_test2, 是一组 trunk 链路 (eth0,eth1), 其中 v_test2 是 VLAN 桥;
- Br_test1, 是一个普通桥, (eth6,eth7)
- Br_test3,v_test4,v_test5, 是一组 trunk 链路 (eth4, eth5), 其中 br_test3 为普通桥,
- v_test4,v_test5 为 VLAN 桥
- Br_test6, 是普通桥 (eth8,eth9)

配置:

1, 为没有 IP 的链路 (br_default 链路默认有 IP), 增加如下静态路由:

桥 IP 所在网段/网段掩码/0.0.0.0/桥接口

192.168.4.0/255.255.255.0/0.0.0.0/v_test4

192.168.5.0/255.255.255.0/0.0.0.0/v_test5 192.168.5.0/255.255.255.0/0.0.0.0/v_test6

2, 若多个链路在同一网段, 则需为多个链路上的每个服务增加如下静态路由:

服务 IP/255.255.255.255/0.0.0.0/桥接口

192.168.5.50/255.255.255.255/192.168.5.254/v_test5 192.168.5.51/255.255.255.255/192.168.5.254/br test6

192.168.0.50/255.255.255.255/192.168.0.254/br_default 192.168.0.51/255.255.255.255/192.168.0.254/br_test1

3, 为每个链路 (非 br_default 桥), 增加如下策略路由:

0.0.0.0/0.0.0.0/桥网段网关/桥接口 (不包括 br_default 桥)

0.0.0.0/0.0.0.0/192.168.0.254/br_test1 0.0.0.0/0.0.0.0/192.168.2.254/v_test2 0.0.0.0/0.0.0.0/192.168.3.254/br_test3 0.0.0.0/0.0.0.0/192.168.4.254/v_test4 0.0.0.0/0.0.0.0/192.168.5.254/v_test5 0.0.0.0/0.0.0.0/192.168.6.254/br_test6

192.168.0.51/255.255.255.255/0.0.0.0/br_test1/策略路由

192.168.2.50/255.255.255.255/0.0.0.0/v_test2/策略路由

192.168.3.50/255.255.255.255/0.0.0.0/br_test3/策略路由

合计:7条静态路由,9条策略路由。