

深空® web 应用防火墙系统

SkyDeep® Web Application Firewall System

Version 1.x 管理员指南

" 网站安全深度防御 "

更新日期: 2013-10

最新信息: <http://www.sky-deep.com>

版权所有© 2013 福州深空®信息技术有限公司

Copyright© 2013 FuZhou SkyDeep Information Technology Co.,Ltd

目录

第一章	欢迎使用 " 深空 WEB 应用防火墙系统 "	- 7 -
第二章	产品术语、部署、原理、安全架构	- 9 -
一、	产品术语	- 9 -
二、	产品部署、原理、安全架构	- 10 -
第三章	快速使用说明	- 11 -
第四章	系统需求、安装与启动	- 12 -
一、	系统需求	- 12 -
二、	安装与启动	- 13 -
第五章	产品管理概述	- 15 -
一、	选择客户端界面语言	- 15 -
二、	连接服务器	- 15 -
三、	一次同时登录多台服务器(批量登录)	- 16 -
四、	正则表达式测试工具	- 17 -
五、	查看所有站点信息	- 17 -
六、	创建私有/删除私有/修改公共或私有 WAF 策略	- 18 -
七、	屏蔽所有私有策略	- 19 -
八、	重载所有策略	- 20 -

第六章 WAF 公共/私有策略 操作	- 21 -
一、 WAF 运行模式	- 21 -
二、 IIS 配置保护策略	- 22 -
三、 策略作用于 HTTPS	- 23 -
四、 WAF 对拦截请求的处理	- 23 -
五、 禁止代理访问策略	- 24 -
六、 IP 访问控制策略(IP 黑/白名单)	- 24 -
七、 IP 访问控制策略(IP 动态白名单)	- 26 -
八、 特权 IP 策略	- 27 -
九、 主动防御策略(IP 访问行为监视)	- 27 -
十、 主动防御策略(URL 访问次数限制)	- 28 -
十一、 防盗链策略	- 29 -
十二、 HTTP 策略(通用头部)	- 29 -
十三、 HTTP 策略(请求头部)	- 30 -
十四、 HTTP 策略(实体头部)	- 30 -
十五、 HTTP 策略(用户自定义头部)	- 31 -
十六、 HTTP 策略(返回头部)	- 31 -
十七、 HTTP 策略(请求方式)	- 32 -
十八、 HTTP 策略(限制头部总长)	- 33 -
十九、 URL 策略(URL 最大长度)	- 34 -
二十、 URL 策略(URL 参数部分最大长度)	- 34 -
二十一、 URL 策略(URL 非参数部分最大长度)	- 34 -

二十二、	URL 策略(URL 非参数部分关键字过滤)	- 35 -
二十三、	URL 策略(URL 参数部分关键字过滤)	- 35 -
二十四、	URL 策略(URL 参数部分关键字过滤-白名单策略)	- 37 -
二十五、	URL 策略(URL 参数部分关键字过滤-黑名单策略)	- 40 -
二十六、	URL 策略(URL 黑名单)	- 40 -
二十七、	URL 策略(特权 URL)	- 41 -
二十八、	URL 策略(URL+IP 限制)	- 41 -
二十九、	URL 策略(URL 请求文件类型限制)	- 42 -
三十、	POST 策略(POST 请求内容关键字过滤)	- 42 -
三十一、	POST 策略(POST 请求 URL 限制)	- 43 -
三十二、	COOKIE 策略(COOKIE 内容关键字过滤)	- 44 -
三十三、	IIS 返回数据策略(HTTP 返回状态码过滤)	- 45 -
三十四、	IIS 返回数据策略(HTTP 返回内容过滤/网页内容过滤)	- 48 -
三十五、	带宽策略	- 49 -
三十六、	动态特权 IP 策略	- 50 -
第七章	制作硬件 WAF	- 54 -
一、	硬件准备	- 55 -
二、	软件准备	- 55 -
三、	部署方式	- 56 -
四、	其它选项说明	- 59 -
第八章	日志类操作	- 61 -

一、	查看日志文件内容	- 62 -
二、	日志文件管理	- 63 -
三、	日志记录对象管理	- 63 -
第九章	产品系统操作	- 65 -
一、	产品客户端登录 IP 限制	- 65 -
二、	产品服务端绑定 IP/端口	- 66 -
三、	系统控制	- 66 -
四、	产品默认行为	- 66 -
五、	用户管理	- 67 -
六、	文件管理	- 68 -
七、	命令行	- 69 -
第十章	不同环境下的注意事项	- 70 -
一、	WINDOWS XP x64 / WINDOWS SERVER 2003 x64 操作系统	- 70 -
二、	IIS7.0 及其以后版本的环境中	- 71 -
三、	WINDOWS VISTA x64 / WINDOWS SERVER 2008 x64 / WINDOWS 7 x64 / WINDOWS SERVER 2012 / WINDOWS 8 x64 操作系统	- 73 -
四、	域控制器 (DOMAIN CONTROLLER) 上的额外操作	- 74 -
第十一章	使用审计策略	- 79 -
一、	启用对象访问审计策略	- 79 -
二、	查看对象访问审计日志	- 80 -

第十二章 卸载产品	- 82 -
一、 卸载前的注意事项	- 82 -
二、 打开卸载程序	- 82 -
三、 开始卸载	- 82 -
第十三章 技术支持及联系方式	- 83 -

第一章 欢迎使用

" 深空 web 应用防火墙系统 "

" 深空 web 应用防火墙系统 " 是由 **福州深空信息技术有限公司** 自主研发而成的,具有完全自主知识产权的 Web 应用防火墙软件产品.

在防御 web 攻击安全策略上,本产品含有: IIS 配置保护、禁止代理访问、IP 访问控制(黑名单、白名单、动态白名单(**抗应用层 CC 攻击,应用层 DDOS 攻击,机器人访问等**))、特权 IP)、IP 访问行为主动防御(**抗应用层 CC 攻击,应用层 DDOS 攻击**)、URL 访问次数主动防御(**抗应用层 CC 攻击,应用层 DDOS 攻击**)、防盗链、HTTP 通用头部各成员长度检查、HTTP 请求头部各成员长度检查、HTTP 实体头部各成员长度检查、HTTP 用户自定义头部各成员长度检查、HTTP 返回头部各成员内容过滤、HTTP 请求方式限制、HTTP 头部总长检查、URL 总长限制、URL 参数部分长度限制、URL 非参数部分长度限制、URL 非参数部分关键字过滤、URL 参数部分关键字过滤 (白名单策略、黑名单策略、自定义放行关键字和自定义强制拦截关键字) 、URL 黑名单检查、特权 URL 检查、URL+IP 访问控制、URL 请求文件类型检查、POST 请求内容过滤、POST 请求的 URL 限制、COOKIE 内容关键字过滤、HTTP 返回状态码过滤、HTTP 返回例外状态码设置、HTTP 返回内容过滤 (网页内容过滤) 、各网站目录每 IP 最大带宽限制,等 30 多种安全策略功能.

在管理上,本产品采用 C/S 架构(Client/Server,客户端/服务端)模式,用户可以通过客户端远程管理服务端,功能上有: 查看/修改/启用/禁用上述安全策略、限制客户端登录的 IP 策略(IP 白名单策略/IP 黑名单策略)、查看/修改产品默认参数(如绑定的 IP,监听的端口,不同情形下 WAF 的相应形式等)、系统控制(重启 IIS、关闭 IIS、重启服务器、关闭服务器)、管理员用户添加/删除/修改/激活/禁用、普通用户添加/删除/修改/激活/禁用/权限设置(本产品的普通用户这一概念可以方便 IDC 用户开设 **Web 防火墙网络安全增值服务**)、产品日志/Web 防火墙拦截日志/管理日志/错误日志 的 查看/删除/下载、日志记录对象管理 (可以只记录指定策略的拦截日志) 、服务器文件管理 (查看/删除文件或文件夹(可批量操作)/新建文件夹/重命名文件或文件夹/上传文件或文件夹(可批量操作)/下载文件或文件夹(可批量操作)) 、命令行模拟 (远程模拟执行 cmd 命令) 等功能.

本产品研制过程中,研发人员与安全研究人员携手,从入侵的角度思虑黑客可能的攻击手法,继而在产品的安全策略中加以拦截限制,提高产品对黑客的“免疫”程度.

本产品研制过程中,研发人员根据网站管理人员对“低管理开销、运行维护价值显性化”的需求,提供了诸如远程策略管理、服务器文件管理、命令行模拟等一系列便利管理功能,充分确保安全与运行维护的高效果和高效率.

" 深空 web 应用防火墙系统 " 提供的业界领先的 Web 应用攻击防护能力,保证了用户 Web 应用系统的连续性与高可靠性,有效地降低了安全风险.

第二章 产品术语、部署、原理、安全架构

一、 产品术语

WAF: Web 应用防火墙(Web Application Firewall),如无特别说明,本指南中特指本 Web 应用防火墙产品.

产品服务端: 指安装完产品后,服务器中的 WAFSvc.exe 进程,简称**服务端**.

产品客户端: 指 WAF-Client.exe 客户端界面程序,简称**客户端**.该程序一般运行于管理员 pc 机中,然后进行远程管理产品运行.出于安全考虑,本产品**客户端**有“**管理员客户端**”和“**普通用户客户端**”这两种.

公共策略: 这是默认策略,有且仅有一个,默认所有站点都使用公共策略.

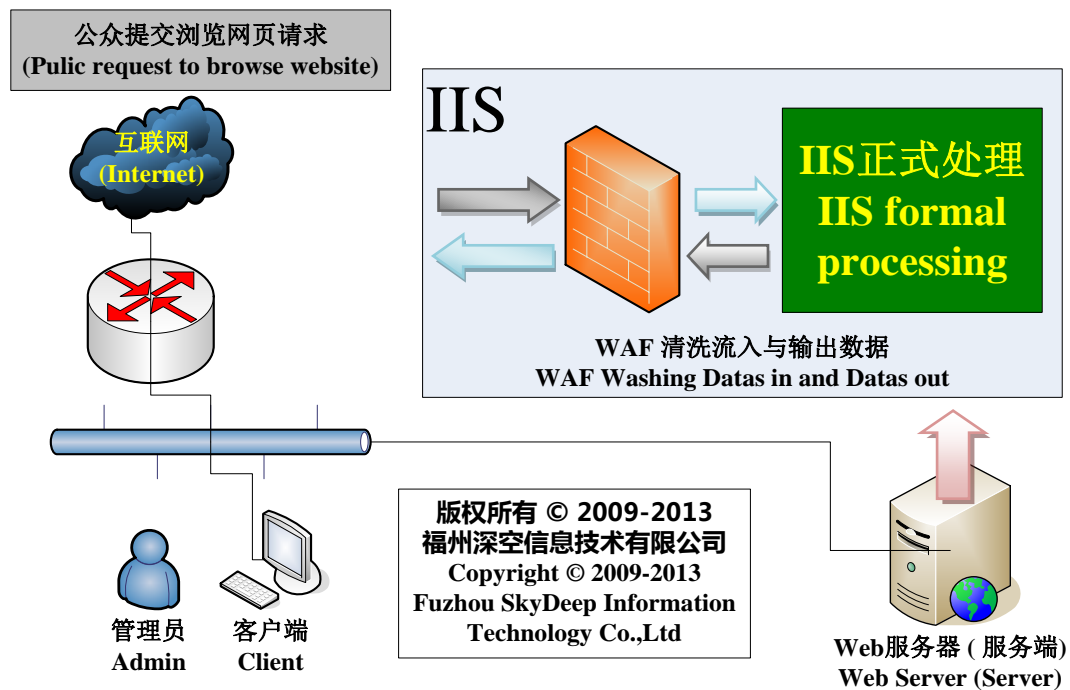
私有策略: 可以有多个,用户对某个站点配置独立的防护策略,这一策略即为私有策略.使用私有策略的站点,其防护策略不受公共策略的影响,除非 **WAF** 配置成“**屏蔽私有策略**”.

屏蔽私有策略: WAF 将忽略所有的私有策略,强制所有站点都使用公共策略.

产品管理员: 对产品具有完全控制权限的用户,简称 管理员 .

普通用户: 只能管理部分私有策略的低权限用户.

二、 产品部署、原理、安全架构



上图所示:

服务端安装在 web 服务器中,用户通过客户端可以远程管理服务端.

服务端在 IIS 中内置安全检测模块,对所有的流入与流出请求作出分析,再裁定是否放行或采取相关动作,这一过程好比“清洗流入与流出 IIS 的数据”。

第三章 快速使用说明

提示:用户可直接观看随本指南一起分发的相关演示视频而无需阅读后文

注意:如果本产品安装在 64 位操作系统上,或者安装在 IIS7.0 及其以后版本的系统中时,或者安装在域控制器 (Domain Controller) 上,在安装产品前,[须进行一些额外配置](#).

第一步:停止 IIS 的运行 (iisreset /stop) ;

第二步:安装**服务端**程序 WAF-Setup.exe,随后按提示操作,直至安装完成;

第三步:重新开启 IIS 的运行(iisreset /start) ;

打开**客户端**,输入服务器的 IP、产品默认的用户名(admin)、产品默认密码 (admin-12345) 连接服务端,开始管理.

完毕.

注意,本产品默认在服务器上开启 20011 端口,如果用户有防火墙,需要开放此端口才能进行远程管理,否则只能进行本地管理(服务器上打开**客户端**连接 127.0.0.1).

如果用户在操作过程中遇到困难,请查阅[技术支持及联系方式](#).

第四章 系统需求、安装与启动

一、 系统需求

1.计算机硬件性能需求：

处理器： Intel Pentium III 以上

内存： 128MB 以上

硬盘： 剩余空间在 100MB 以上

2.操作系统需求(32 位/64 位)

Windows 2000

Windows XP Professional

Windows Server 2003

Windows Vista Ultimate

Windows Server 2008

Windows 7 Ultimate

Windows Server 2008 R2

Windows 8

Windows Server 2012

使用虚拟化技术后继续支持下列平台(32 位/64 位):

Asianux

CentOS

Debian GNU/Linux	Fedora
FreeBSD	Java Desktop System
Mandrake Linux	NetWare
openSUSE	Oracle Enterprise Linux 5
Oracle Linux	Red Hat Enterprise Linux
Red Hat Linux	Solaris
SUSE Linux	SUSE Linux Desktop
SUSE Linux Enterprise	Turbolinux
Ubuntu	

二、 安装与启动

注意:如果本产品安装在 64 位操作系统上,或者安装在域控制器 (Domain Controller) 上,在安装产品前,[须进行一些额外配置](#).

第一步:将产品安装光盘放入光驱中,然后双击光盘根目录下的产品安装程序 WAF-Setup.exe,仔细阅读弹出对话框中的 " 最终用户许可协议 " ,如果不同意该协议,则点击 " 不同意/退出(Exit) " 退出安装.如果同意该协议,则勾选 "我已认真阅读并同意上述协议" ,然后点击 " 同意/下一步(Next) " ,继续后面的步骤.

第二步:停止 IIS 的运行,选择安装目录,然后点击 " 开始安装 (Install) ",随后等待安装完成即可关闭窗口,如下图所示 :

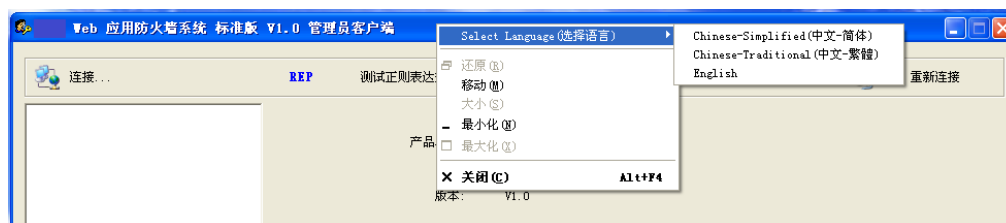


第三步:开启 IIS 的运行.

第五章 产品管理概述

一、 选择客户端界面语言

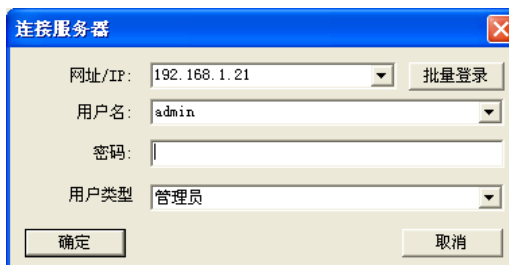
用户可根据自身情形,选择适合自己的客户端界面语言.操作方法是:打开客户端,关闭登录框,然后在客户端窗口的标题栏中点击右键,即可选择客户端语言.如下图所示:



选择新的语言后,重新打开客户端即可生效.

二、 连接服务器

打开客户端,连接服务器,输入相关信息(默认用户名:admin,默认密码:admin-12345):



注意:第一次登录后,请立即在 " 产品系统 " -> " 用户管理 " 中修改默认用户名和默认密码.

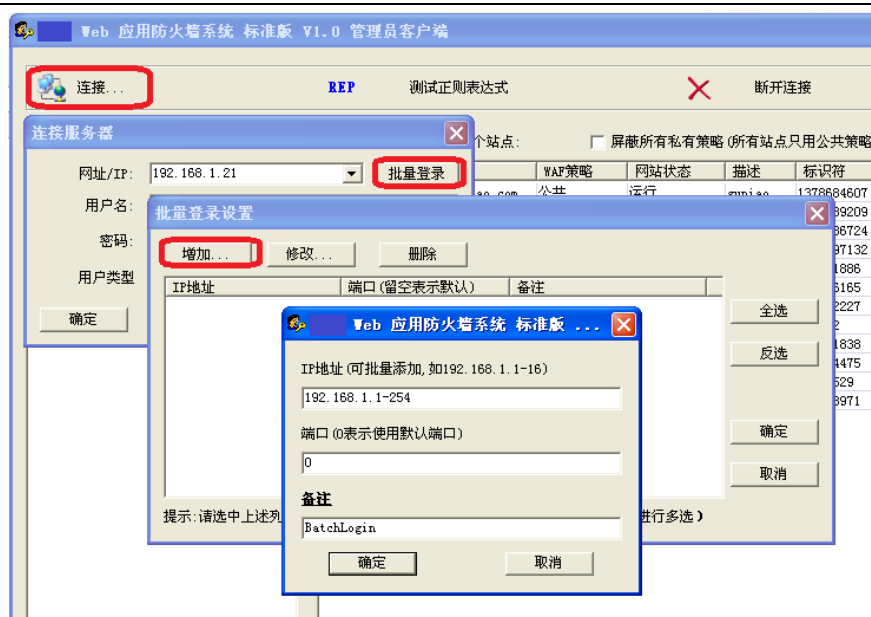
提示:本产品客户端和服务端之间的通信已经加密,而且在客户端登录时使用 **NTLM** 技术进行认证,因而可以防止第三方从网络中嗅探密码。

登录后可以看到类似如下图所示的管理界面,左边为**树形列表区**,右边为**信息显示区**。



三、一次同时登录多台服务器(批量登录)

用户可以同时连接其它单个服务器,也可以使用批量登录,一次同时连接多达 254 个服务器,如下图所示:



四、 正则表达式测试工具

客户端提供了测试正则表达式的简易工具,在工具栏中点击“测试正则表达式”,用户可以输入正则表达式和测试文本来调试正则表达式,如下图所示:



注:本产品中使用的正则表达式遵从 **Visual Basic 正则表达式语法**.

五、 查看所有站点信息

信息显示区中,用户可以看到当前服务器上的所有站点的相关信息,包括:网

站总数、网站运行状态、网站名称、网站根目录、绑定的 IP 地址、网站绑定的端口、网站对应的域名、网站标识符、WAF 策略、HTTPS 端口等信息。

六、 创建私有/删除私有/修改公共或私有 WAF 策略

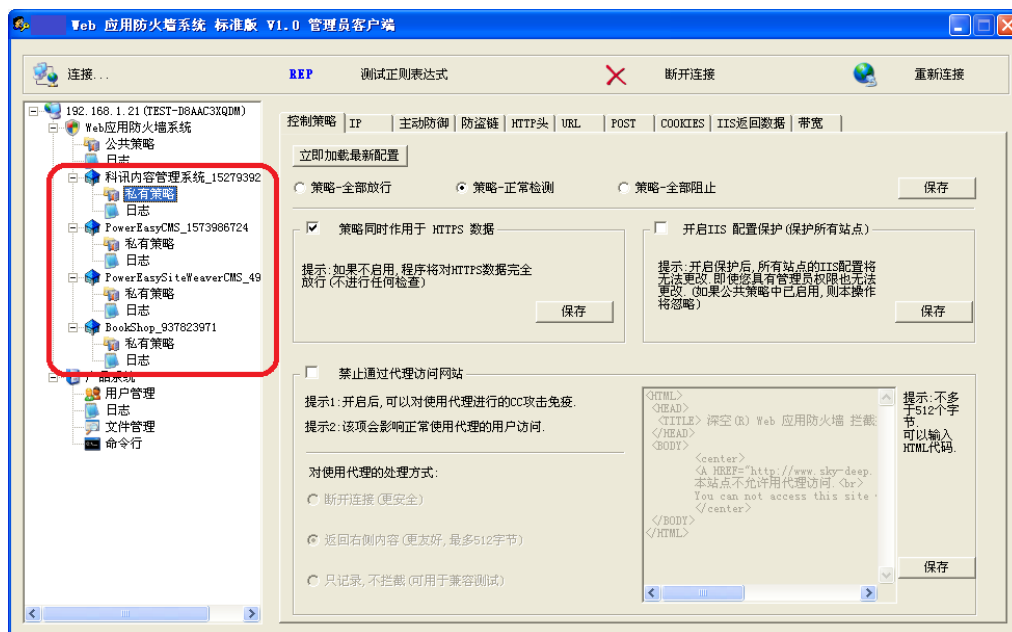
普通的 Web 应用防火墙,如论是软件还是硬件,其策略都是只能作用于所有的站点,如果某台服务器中含有大量的不同类型的站点,则用一种拦截策略去防御所有类型的站点就经常会遇到兼容性严重下降等问题。

例如,假设某台服务器上有 www.123.com 和 www.456.com 这两个站点,其中,前者的站点在 URL 参数部分中需要拦截 “--” 等 SQL 注入关键字,而后者的站点它本身正常的 URL 参数部分中就含有 “--” 关键字.这时,如果策略中拦截了 “--” 关键字就势必影响后者的站点正常工作,而如果不拦截 “--” 关键字,则前者的站点就很有可能暴露于 SQL 注入的危险之中。

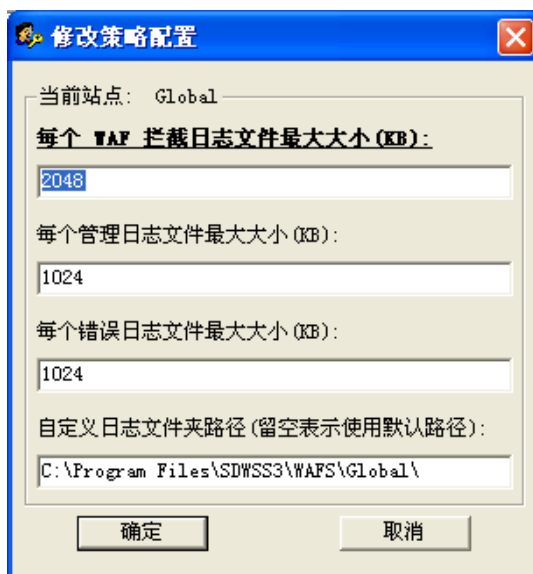
用户通过使用本产品的“私有策略”这一新概念,可以对此情形应付自如。

信息显示区中,管理员用户通过“使用私有策略”/“删除”按钮,可以给单个站点设置 使用/删除 独立的 WAF 策略(私有策略).这样设置后,该站点将使用自己独立的 WAF 策略 (私有策略),不受公共策略 (除非管理员用户开启了“屏蔽所有私有策略”)和其它私有策略的影响。

如下图所示创建了 4 个私有策略,每一个私有策略都对应一个站点:



信息显示区中,用户通过“修改”按钮,可以设置公共策略/私有策略的各类日志文件单个最大大小和日志文件夹路径,如下图所示。



提示:根据版本的不同(如企业版,标准版,高级版等),用户可创建的最多私有策略的个数也不同。

七、 屏蔽所有私有策略

信息显示区中,用户通过“屏蔽所有私有策略”按钮,可以使得 WAF 忽略所有

的私有策略,强制所有站点使用公共策略.

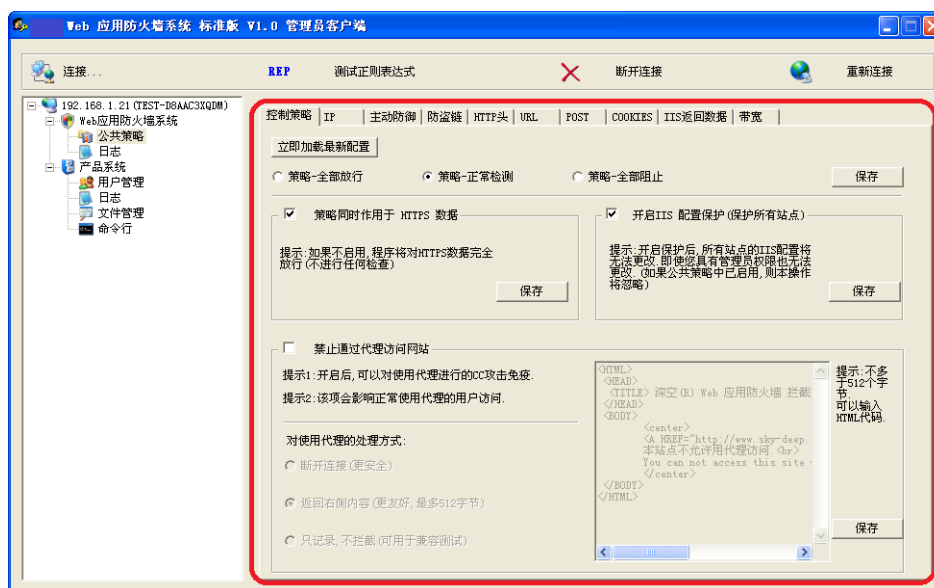
注意:此功能需点击“重载所有策略”后方能生效.

八、 重载所有策略

信息显示区中,用户通过“重载所有策略”按钮,可以使 WAF 立即重新加载公共策略和所有的私有策略.

第六章 WAF 公共/私有策略 操作

本章介绍的是 产品客户端->左边树形列表->Web 应用防火墙系统->公共/私有策略 的操作,各子策略对应的界面在右边的信息显示区中.



用户亦可观看随本指南一起分发的相关演示视频而无需阅读后文.

商业版用户如果在操作中遇到困难,可以[查看最后一章以寻求技术支持](#).

一、 WAF 运行模式

本产品提供了如下三种 WAF 的运行模式:

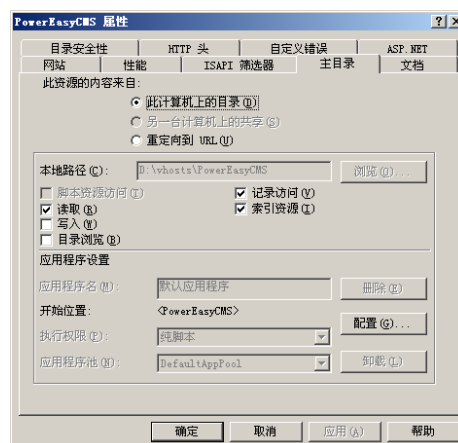
- 策略-全部放行:** WAF 放行所有请求,不进行任何安全检测.
- 策略-正常检测:** WAF 根据用户配置的相关安全策略,对流入与流出 IIS 的数据进行正常检测与清洗.
- 策略-全部阻止:** WAF 阻止所有的请求.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二、 IIS 配置保护策略

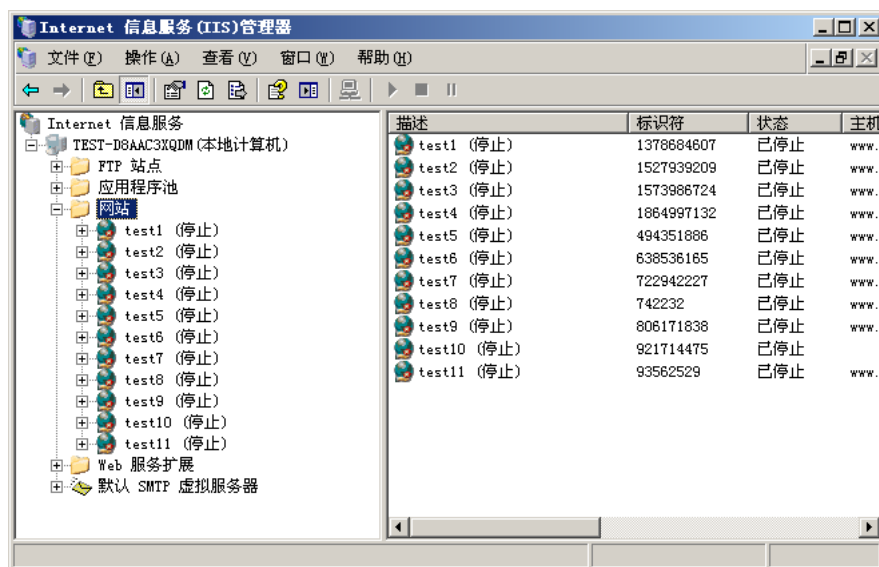
本产品提供的 IIS 配置保护功能实现了对 IIS 配置数据的防篡改,启用保护后,受保护站点的 IIS 配置数据(如,网站名称、网站根目录、默认首页文档、应用程序池、筛选器列表等)将无法被篡改,即使恶意用户具有操作系统管理员权限.

下图显示了在“公共策略”中开启了“IIS 配置保护”后,以操作系统的 Administrators 组成员的身份打开 inetmgr.msc,即 Internet 信息服务(IIS)管理器,然后任选一个站点,查看其 **属性** 信息的情形.从图中可以发现,相关属性都已经灰化而不可更改.



提示：如果在“公共策略”中开启了“IIS 配置保护”,则 IIS 中所有站点的配置都同时得到了保护.如果在某个“私有策略”中开启了“IIS 配置保护”,则只有这个私有策略对应站点的 IIS 配置才能防篡改.

注意：开启“IIS 配置保护”后,网站正常运行将不受影响,但 IIS 将无法更新网站状态信息,因此用户在 IIS 管理器中查看站点状态时,将可能看到类似如下图所示信息,虽然此时网站实际是正常运行:



警示：当用户卸载产品前,用户应该确保公共策略和各私有策略中的 IIS 配置保护已取消,否则产品卸载后,用户依然会无法更改站点的 IIS 配置信息。

三、 策略作用于 HTTPS

本产品可以供用户选择是否对 HTTPS(Secure Hypertext Transfer Protocol),即安全超文本传输协议 的数据进行安全检测。

警示：如果不开启,则 WAF 对 HTTPS 类的数据全部放行。

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效。

四、 WAF 对拦截请求的处理

WAF 对拦截请求的处理,用户有三种处理方式可以选择:

- 断开连接(更安全):** 立即断开连接。
- 向浏览者发送指定信息:** 比如向浏览者发送“拒绝访问”等文字。
- 只记录,不拦截(可用于兼容测试):** WAF 记录下所有不合策略的请求但不拦截.本方式可以用来测试当前策略和网站的兼容程度,这期间网站的

正常运行不受影响,用户可以逐步调试策略,直至满意为止.

五、 禁止代理访问策略

如果开启本策略,WAF 将对通过代理访问的浏览请求进行拦截.

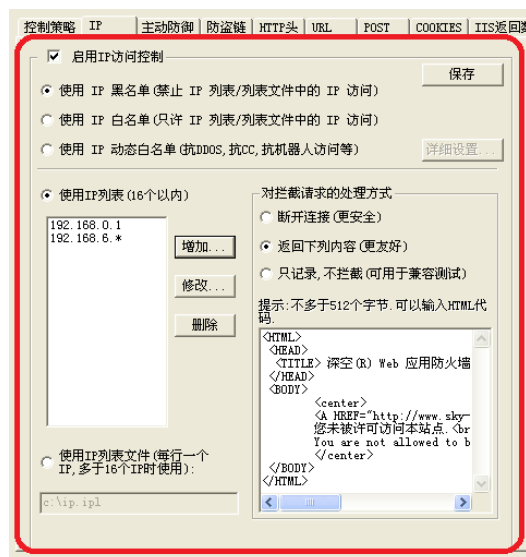
保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

六、 IP 访问控制策略(IP 黑/白名单)

如果开启本策略,而且选择 **IP 黑名单**策略,则 WAF 将对黑名单中的 IP 进行屏蔽,被屏蔽的 IP 将无法访问任何页面.

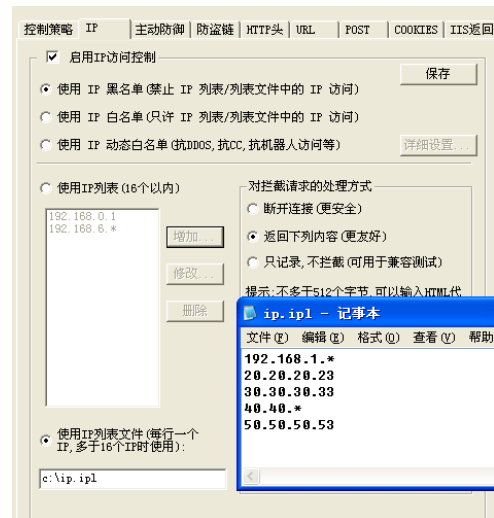
如果开启本策略,而且选择 **IP 白名单**策略,则 WAF 将只允许白名单中的 IP 访问,非白名单 IP 都将被屏蔽,被屏蔽的 IP 将无法访问任何页面.

如果黑/白名单 IP 的个数不超过 16 个,则用户可以在客户端中设置具体的 IP,可以使用星号通配符,如下图所示:



如果黑/白名单 IP 的个数超过 16 个,则必须使用 IP 列表文件,并在客户端中配置 IP 列表文件的全路径.IP 列表文件中每一行配置一个 IP,可以使用星号通配符,

如下图所示:



提示:IP 列表文件的拓展名必须是 .ipl

提示:如果用户具有网站合法浏览者的 IP 地址列表,并把这些 IP 地址写入 IP 列表文件中(如果合法者 IP 超过 16 个时),然后使用这里提及的 IP 访问控制白名单策略,则可以极大地提升网站的安全性.

警示：用户必须确保黑/白名单 IP 列表文件存在,而且拓展名为.ipl,否则将无法保存配置,或者 WAF 将无法正常运行.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

七、 IP 访问控制策略(IP 动态白名单)

IP 动态白名单

IP动态白名单 (抗DDOS, 抗CC, 抗机器人访问等):
提示: 用户可以参考管理员/用户指南了解详细原理与用法.

非白名单中的 IP 访问控制

非白名单中的IP允许访问的URL (及其子URL)
作用: 使非白名单中的 IP 有机会通过访问本设置中的 URL 而成为白名单中的 IP

把非白名单 IP 的请求重定向到下面的 URL .

白名单 IP 文件 (拓展名必须是 .ipl)

白名单 IP 文件全路径 (注意: 文件必须存在):

每隔 秒读取一次白名单 IP 文件 (最小值为3)

每隔 分钟清空一次白名单 IP 文件 (最小值为1)

如果开启本策略,而且选择 **IP 动态白名单**策略,则受保护站点将具备**抵御应用层 CC 攻击,抵御应用层 DDOS 攻击,抵御机器人访问,防盗链**等能力.

IP 动态白名单是 WAF 和网站应用互动的一种模式.此时,WAF 使用 IP 白名单策略,初始时 IP 白名单列表为空,随后 WAF 每隔一定时间(如每隔 3 秒)读取指定 IP 列表文件中的 IP 并更新到 IP 白名单列表中.

用户可以在网站中设置一个验证页面(如 /Dynamic_White_IP/asp/default.asp),把经过验证的(比如:能正确输入验证码的/能正确回答问题的 等)IP 写入指定文件中(每行一个 IP),如: C:\Web\ Dynamic_White_IP\asp\IP.ipl .然后 WAF 每隔一定时间(如每隔 3 秒)读取一次这个 IP.ipl 文件,并更新到 WAF 内部的 IP 白名单列表中,随后这个经过验证的 IP 就可以正常浏览网站.

对任意一个未经验证的 IP(WAF 内部的 IP 白名单列表中无此 IP 记录),无论访问任何页面,都会被自动重定向到验证页面中(如 /Dynamic_White_IP/asp/default.asp).

对已经经过验证的 IP(WAF 内部的 IP 白名单列表中存在此 IP 记录),其可正常浏览站点,不再受本策略限制.

警示 :用户必须确保动态白名单 IP 列表文件存在,而且拓展名为 .ipl,否则将无法保存配置,或者 WAF 将无法正常运行.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

八、 特权 IP 策略

如果开启本策略,则特权 IP 列表中的 IP 将**不受任何 WAF 策略限制**.WAF 将对特权 IP 的流入/流出数据完全放行.

警示 :由于特权 IP 不受任何 WAF 策略限制,所以用户应对特权 IP 列表中的成员进行严格审核.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

九、 主动防御策略(IP 访问行为监视)

The screenshot displays the configuration page for the '主动防御-IP访问行为限制' (Active Defense - IP Access Behavior Monitoring) strategy. The page includes tabs for different defense types and a main configuration area with several sections:

- 启用策略 (Enable Strategy):** A checkbox is checked, indicating the strategy is active. A '保存' (Save) button is present.
- 对违规的 IP 在 (For violating IP):** A setting to ban IP addresses for 600 seconds.
- 对同一 IP 地址 (For the same IP address):** A checkbox is checked, with settings for 10 seconds and 20 requests.
- 对同一 IP 地址 (For the same IP address):** A checkbox is checked, with settings for 3 seconds and 48 requests.
- 对拦截请求的处理方式 (Handling of intercepted requests):** Three options are available: '断开连接 (更安全)' (Disconnect, safer), '返回下列内容 (更友好)' (Return the following content, friendlier), and '只记录,不拦截 (可用于兼容测试)' (Only record, no interception, for compatibility testing). The 'Return the following content' option is selected.
- HTML Content:** A text area containing the HTML response for blocked requests, including a title and a message in Chinese and English.
- 提示 (Hint):** A note on the right side stating that the HTML content should not exceed 512 characters.

如果开启本策略,WAF 可以对每一个 IP 的访问行为进行监视与统计,因而受

保护站点将具备一定的**抵御应用层 CC 攻击,抵御应用层 DDOS 攻击,抵御机器人访问**等能力.

本策略具体分为**访问频率监视**和**访问不存在页面的频率监视**这两种.

由于黑客攻击网站时,通常会使用各种 web 漏洞扫描软件对网站进行快速的扫描,如 SQL 注入工具频繁对某一页面或多个页面进行快速地 SQL 注入请求,网站文件刺探工具每秒尝试猜测数十个甚至上百个不存在的页面 等.

因此,通过**访问频率监视**和**访问不存在页面的频率监视**,WAF 能够对各类恶意扫描 IP 进行事前主动拦截防御--在指定时间内屏蔽该 IP 的访问.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十、 主动防御策略(URL 访问次数限制)



如果开启本策略,WAF 可以监视与限制指定 URL 每秒最大被请求的次数,因而受保护站点将具备一定的**抵御应用层 CC 攻击,抵御应用层 DDOS 攻击,抵御机器人访问**等能力.

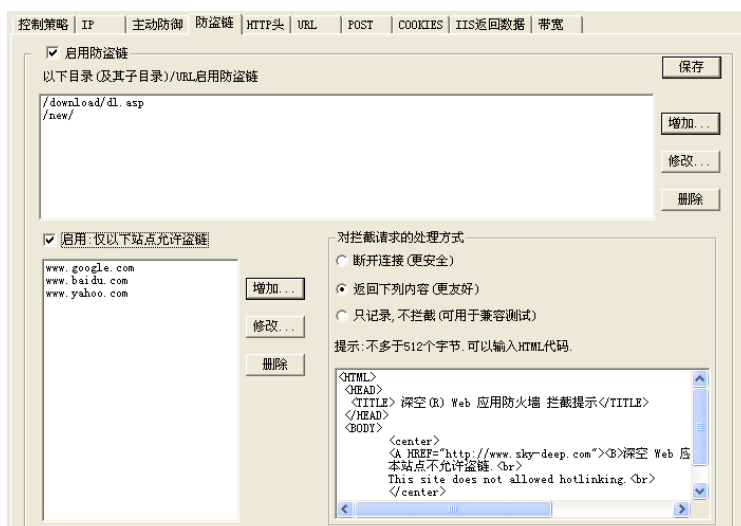
例如在 CC 攻击中,攻击者会对网站中执行时间较长的页面(如论坛网站中的

数据查询页面等)进行频繁地请求,据此不断消耗服务器的资源,最终造成网站无法正常工作.

通过设置 URL 访问次数限制,WAF 将确保受限制的 URL 每秒最多只有指定次数的请求,超出的部分都将被屏蔽.例如对某页面限制每秒最多有 10 次的请求,则在一秒内,前 10 次的请求都不拦截,第 11 次以后的请求都将被屏蔽.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十一、防盗链策略

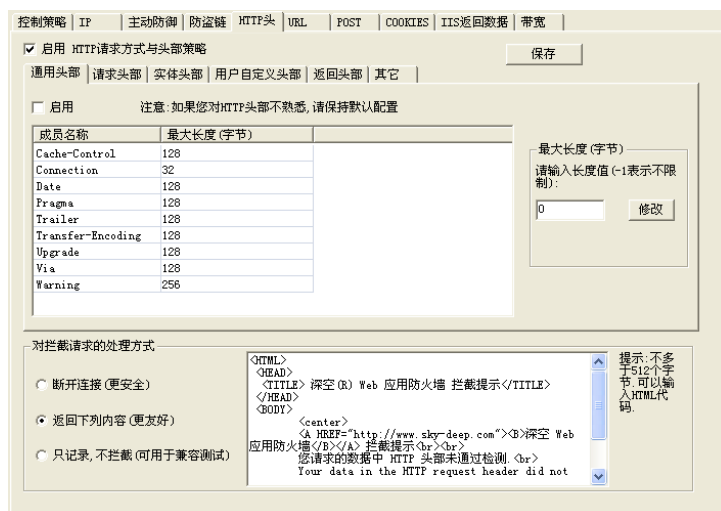


如果开启本策略,WAF 将对指定 URL 的请求进行检测是否是盗链.同时,用户还可以设置允许盗链的站点,如各类搜索引擎,友情站点等.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十二、HTTP 策略(通用头部)

提示:如果用户对 HTTP 协议不熟悉,请保留默认配置.



如果开启本策略,WAF 将对 HTTP **通用头部** 的各成员长度进行检查,如有某成员长度超出限制的最大值,则立即对请求进行拦截.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十三、 HTTP 策略(请求头部)

提示:如果用户对 HTTP 协议不熟悉,请保留默认配置.

如果开启本策略,WAF 将对 HTTP **请求头部** 的各成员长度进行检查,如有某成员长度超出限制的最大值,则立即对请求进行拦截.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十四、 HTTP 策略(实体头部)

提示:如果用户对 HTTP 协议不熟悉,请保留默认配置.

如果开启本策略,WAF 将对 HTTP **实体头部** 的各成员长度进行检查,如有某成员长度超出限制的最大值,则立即对请求进行拦截.

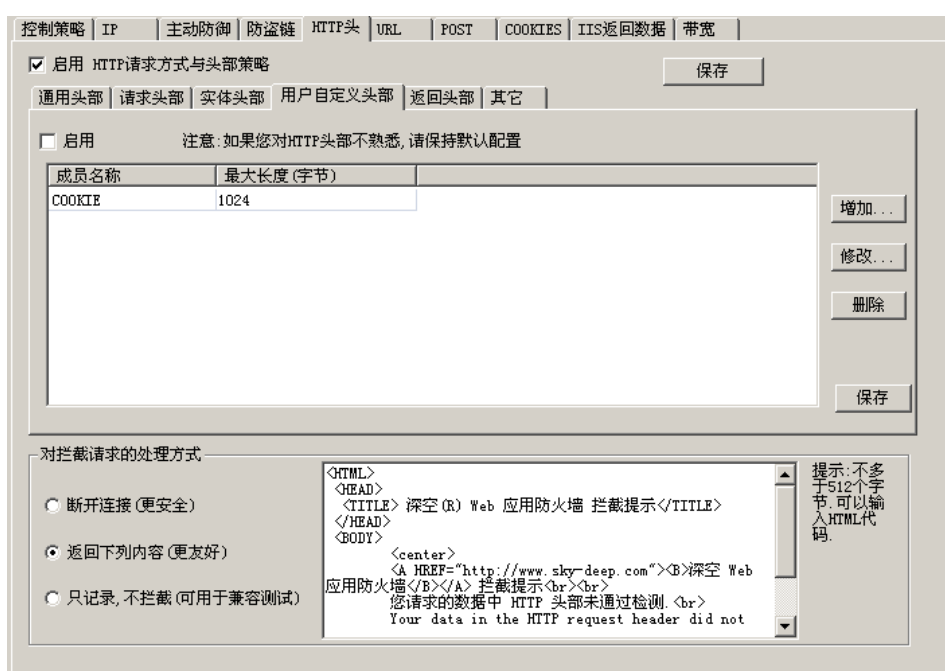
保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十五、 HTTP 策略(用户自定义头部)

提示:如果用户对 HTTP 协议不熟悉,请保留默认配置.

如果开启本策略,WAF 将对 HTTP 用户自定义头部的各成员长度进行检查,如有某成员长度超出限制的最大值,则立即对请求进行拦截.

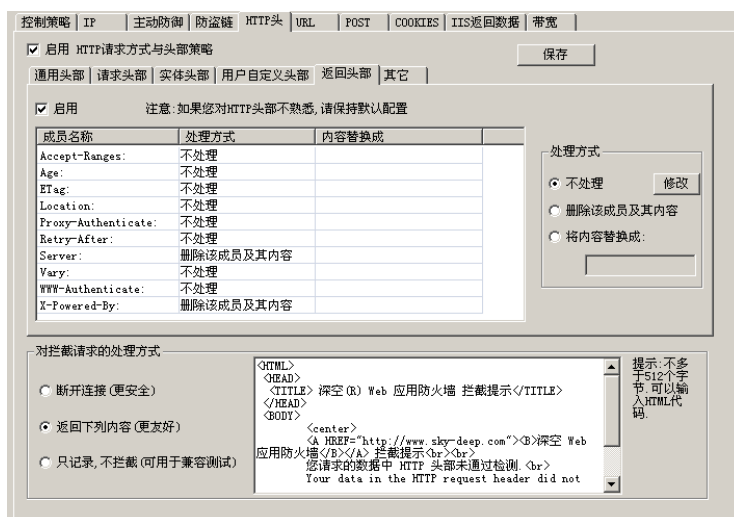
在**用户自定义头部**中,用户可以自定义增加需要限制最大长度的成员名称及其限定值,如下图所示增加限制 COOKIE 成员的最大长度为 1024 个字节:



保存本策略配置后,点击“控制策略” -> “立即加载最新配置” 后方能生效.

十六、 HTTP 策略(返回头部)

提示:如果用户对 HTTP 协议不熟悉,请保留默认配置.



如果开启本策略,WAF 将对 **HTTP 返回头部** 的各成员长度进行安全过滤,如替换其内容/删除成员及其内容等.

通常,在**返回头部**中,一般会泄漏服务器的一些敏感信息,这些敏感信息可被黑客利用来识别服务器的操作系统和 Web 服务软件.

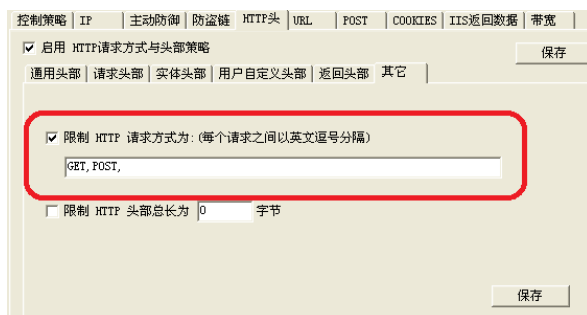
因此,WAF 过滤一些敏感成员,如 **Server** 成员、**X-Powered-By** 成员的内容,将增加黑客收集服务器信息的难度.

用户可以在此设置对各**返回头部**成员的处理方式,如:删除成员及内容,替换返回内容等.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十七、 HTTP 策略(请求方式)

提示:如果用户对 HTTP 协议不熟悉,请保留默认配置.



如果开启本策略,WAF 将对 HTTP **请求方式** 进行检查,只允许用户设置的请求方式,其它一律进行拦截.

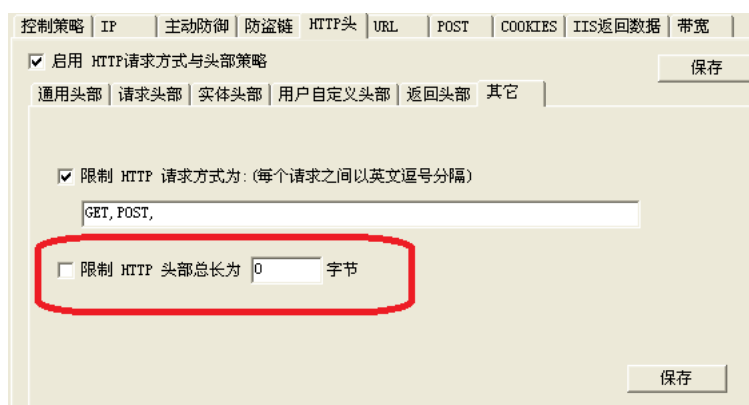
HTTP **请求方式** 如 GET,POST,HEAD,OPTION,DELETE,PUT 等,标记了一个 HTTP 请求的在对应的 URL 上所执行的方式,其中 PUT 和 DELETE 是两个对服务器比较危险的请求方式.

提示:根据 RFC2616 文档,请求方式是大小写敏感的,通常都为大写.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十八、 HTTP 策略(限制头部总长)

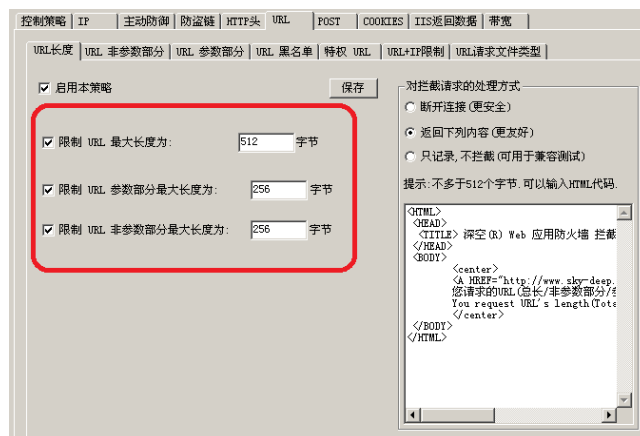
提示:如果用户对 HTTP 协议不熟悉,请保留默认配置.



如果开启本策略,WAF 将对 HTTP 头部总长 进行限制,如果 HTTP 头部总长超过限制,则 WAF 将对请求进行拦截.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

十九、 URL 策略(URL 最大长度)



如果开启本策略,WAF 将对 URL 总长进行限制,如果 URL 总长超过限制,则 WAF 将对请求进行拦截.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二十、 URL 策略(URL 参数部分最大长度)

URL 参数部分是指 URL 中第一个问号后的全部内容,例如 URL:

`/news/news.asp?id=100&update=2011`

URL 参数部分为上面的红色部分.

如果开启本策略,WAF 将对 URL 参数部分的长度进行限制,如果 URL 参数部分的长度超过限制,则 WAF 将对请求进行拦截.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二十一、 URL 策略(URL 非参数部分最大长度)

URL 非参数部分是指 URL 中第一个问号前的全部内容,例如 URL:

`/news/news.asp?id=100&update=2011`

URL 非参数部分为上面的红色部分.

如果开启本策略,WAF 将对 URL 非参数部分的长度进行限制,如果 URL 非参数部分的长度超过限制,则 WAF 将对请求进行拦截.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二十二、 URL 策略(URL 非参数部分关键字过滤)

URL 非参数部分是指 URL 中第一个问号前的全部内容,例如 URL:

/news/news.asp?id=100&update=2011

URL 非参数部分为上面的红色部分.

如果开启本策略,WAF 将对 URL 非参数部分进行关键字过滤.

提示:本产品自带的 URL 非参数部分关键字,将能使 WAF 对利用 IIS 文件拓展名等漏洞进行攻击的请求进行拦截.

用户可以设置**原始匹配关键字**(每个关键字最长 16 字节)和**正则表达式匹配关键字**(每个关键字最长 64 字节)这两种,且都不区分大小写,WAF 检测关键字时,将分别检测原始匹配的关键字和正则表达式匹配的关键字.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二十三、 URL 策略(URL 参数部分关键字过滤)

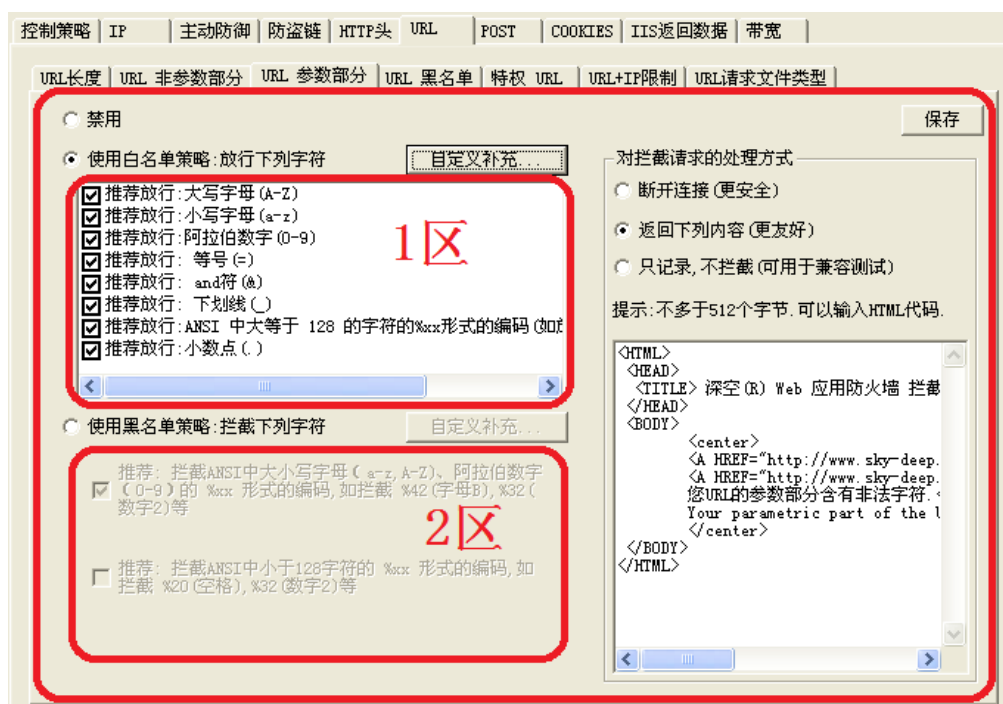
URL 参数部分是指 URL 中第一个问号后的全部内容,例如 URL:

/news/news.asp?id=100&update=2011

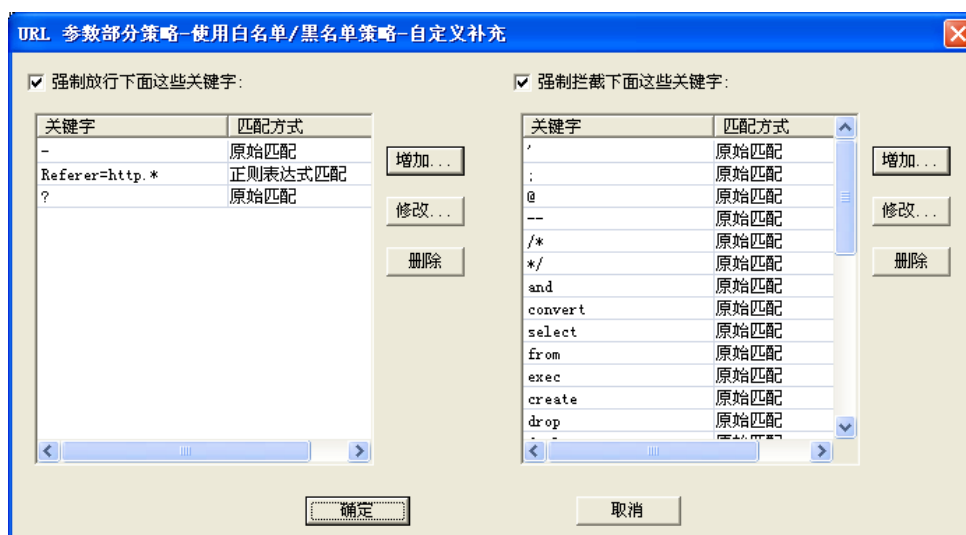
URL 参数部分为上面的红色部分.

由于 URL 参数部分是黑客进行 SQL 注入和跨站等攻击的重点,因此本产品提

供了 **白名单关键字策略** 和 **黑名单关键字策略** 这两种防御方式,并自带了部分关键字,如下图所示:



每种防御方式用户都可以进行 **自定义补充**,自定义补充包括**强制拦截的关键字**和**强制放行的关键字**,其中**强制拦截的关键字**列表中已经定义了一些常见的SQL注入攻击关键字,如下图所示:



关键字匹配方式分为:**原始匹配关键字**(每个关键字最长 16 字节)和**正则表达式匹配关键字**(每个关键字最长 64 字节)这两种,且匹配时都不区分大小写。

WAF 内部对 URL 参数部分的检测顺序依次为:

如果使用**白名单策略**,则:

1. WAF 检测 URL 参数部分是否存在 **强制拦截的关键字** (如果有启用), 如果有,就立即拦截请求.
2. WAF 检测 URL 参数部分是否存在 **白名单之外** (上图中 “1 区” 定义的字符之外)的字符,如果有,就检测是否是 **强制放行的关键字** (如果有启用),如果是,就跳过对该关键字的拦截,否则就立即拦截请求.

如果使用**黑名单策略**,则:

1. WAF 检测 URL 参数部分是否存在 **强制拦截的关键字** (如果有启用), 如果有,就立即拦截请求.
2. WAF 检测 URL 参数部分是否存在 **黑名单之中** (上图中 “2 区” 定义的字符)的字符,如果有,就检测是否是 **强制放行的关键字** (如果有启用),如果是,就跳过对该关键字的拦截,否则就立即拦截请求.

保存本策略配置后,点击 “控制策略” -> “立即加载最新配置” 后方能生效.

二十四、 URL 策略(URL 参数部分关键字过滤-白名单策略)

如果用户网站中 URL 的参数部分出现的**字符比较单一**,或者**格式比较固定**,则推荐使用白名单策略.

举例一:网站中的含参数部分的 URL 都是形如:

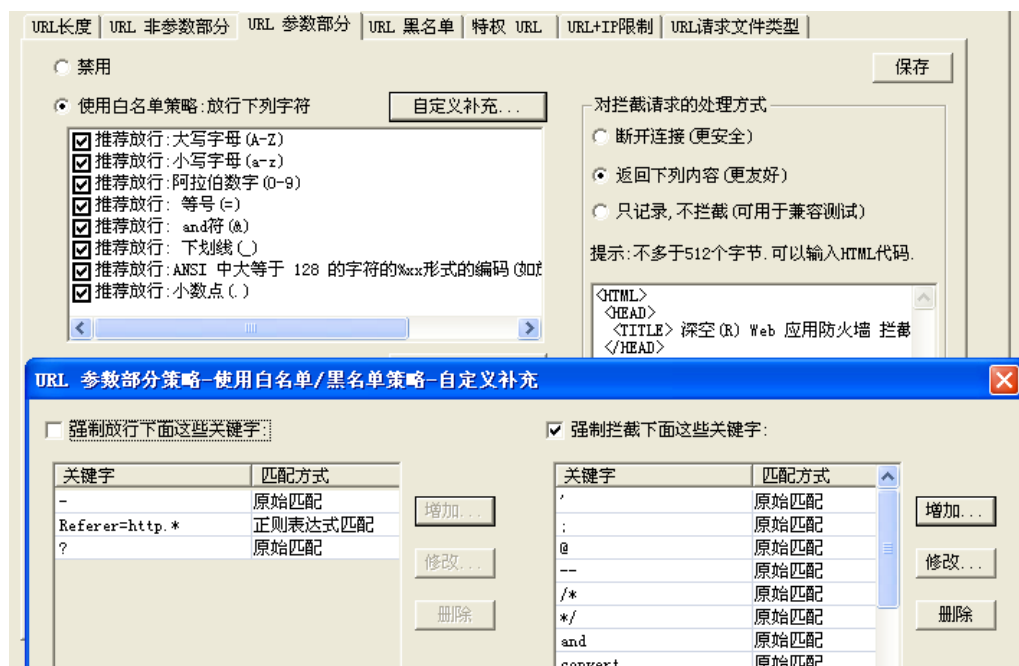
/news/news.asp?id=100&时间=2011-2

/admin/admin_news_add.asp?i_D=1_0_0&Id2=1_0_0&i 未来 3=世界

/book/book.asp?view=fa-sdf-as

分析:参数部分格式比较繁杂,但出现的字符比较单一,可以用:大小写字母(a-z,A-Z),阿拉伯数字(0-9),and 符号(&),减号(-),下划线(_),等号(=),中文 这些范围来描述,而且,单凭这些字符,黑客无法构造出有效的攻击语句,因为 SQL 注入/跨站脚本语句需要生效,一个很关键的就是需要在 URL 参数部分中输入**空格**和**特殊字符**。(提示:对**空格**,黑客在 SQL 注入攻击时可以使用**闭合的注释符**代替,如/****/ 来代替空格)

因此,这里可以使用 白名单策略+产品自带的**自定义强制拦截关键字**,如下图
所示:



提示:本产品推荐用户积极开启使用产品自带的**自定义强制拦截关键字**。

警示:使用白名单关键字的用户在自定义**强制放行的关键字**时,需认真考虑放行该关键字是否会带来安全风险。

一些常见的危险字符有： 星号(*),小于号(<),大于号(>),at 符号(@),单引号

(),分隔符(|),加号(+),空格(),左括号((),右括号()).

举例二:网站中的含参数部分的 URL 都是形如:

/news/news.asp?id=100&update=2011

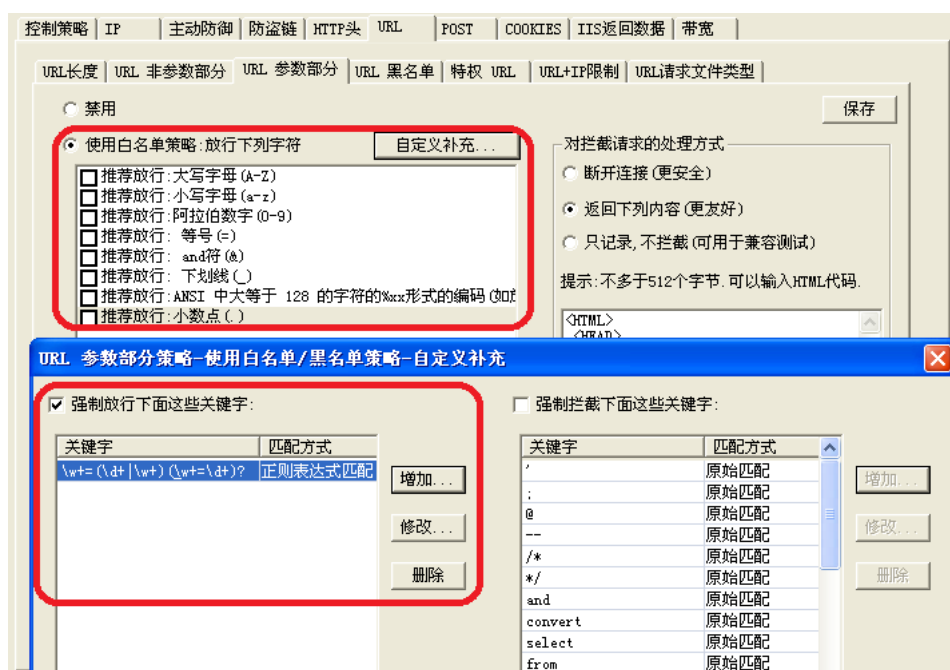
/admin/admin_news_add.asp?id=100

/book/book.asp?view=fasdfas

分析:参数部分格式比较统一,可以用正则表达式加以描述,因而可以使用 白名单策略+**强制放行指定的正则表达式关键字**.

如下所示,自带的白名单关键字可以一个不选,然后点击“自定义补充”,只启用“放行下面这些关键字”,然后加入一个正则表达式关键字:

$\backslash w+=\backslash d+|\backslash w+)(\&\backslash w+=\backslash d+)?$



这样设置后被保护站点的 URL 参数部分的格式将被“定死”,URL 参数部分中只有符合**强制放行关键字**中正则表达式的才被放行,其它一律拦截,因此大大降低了被 SQL 注入/跨站等攻击的危险.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

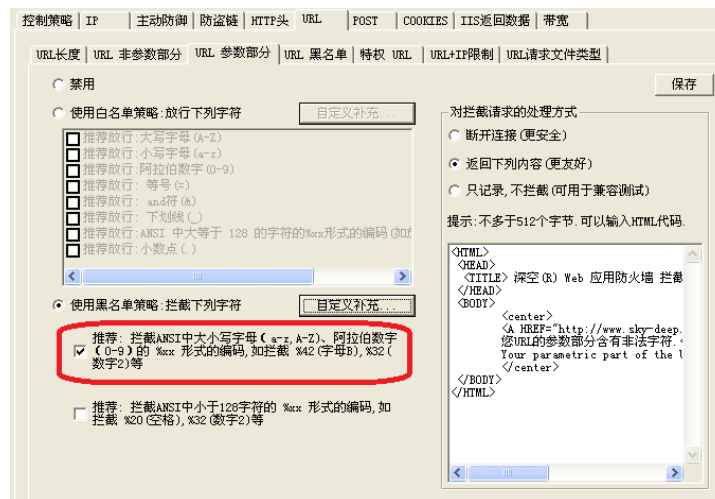
二十五、 URL 策略(URL 参数部分关键字过滤-黑名单策略)

如果用户网站中 URL 的参数部分格式不固定,形式多种多样,或者出现的字符比较繁杂,则推荐使用黑名单策略以实现 WAF 和网站正常应用的最大兼容.

提示:在使用黑名单策略时,推荐用户积极开启使用产品自带的**自定义强制拦截关键字**,该列表中已经定义了一些常见的 SQL 注入攻击关键字.

提示:推荐用户把产品内置的“拦截大小写字母、阿拉伯数字 0-9 的%xx 形式的编码”的黑名单策略开启.该策略可以拦截黑客通过编码变形来试图绕过关键字检测的攻击.

如下图所示:



保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二十六、 URL 策略(URL 黑名单)

如果开启本策略,WAF 将屏蔽所有对处于黑名单中的 URL 及其子 URL(子目

录)的请求.

本策略可用于保护含有重要文件的目录(如数据库文件所在的目录)不被公众访问甚至下载.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二十七、 URL 策略(特权 URL)

如果开启本策略,WAF 将跳过对特权 URL 及其子 URL(子目录)请求的 URL 类策略检查.

本策略可用于对网站中个别特殊的与 URL 类策略冲突的 URL 进行例外处理.

警示:特权 URL 不受 URL 类策略限制,用户应自己确保特权 URL 的安全性,WAF 对特权 URL 不进行 URL 类策略检查(如不进行参数部分关键字检查,不进行非参数部分关键字检查等),因此用户在添加特权 URL 时应当非常谨慎.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二十八、 URL 策略(URL+IP 限制)

如果开启本策略,WAF 将对指定的 URL 限制 IP 访问,只有允许访问的 IP 方能访问该 URL 及其子 URL(子目录).

本策略可用于保护敏感目录(如网站管理后台所在的目录,数据库文件所在的目录等)不被未授权 IP 访问.

提示:用户可以对一个 URL 最多配置 8 个可以访问的 IP 或 IP 段(使用星号(*)通配符).

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

二十九、 URL 策略(URL 请求文件类型限制)

如果开启本策略,WAF 将对所有请求进行请求文件类型检查,只允许用户设置的文件类型被请求,其它一律拦截.

本策略可用于保护敏感文件(如数据库文件.mdb、密码文件.psw 等)不被公众访问甚至下载,也可用于拦截一些特殊拓展名的 webshell(网页后门),如.asa、.cer、.cdx 等.

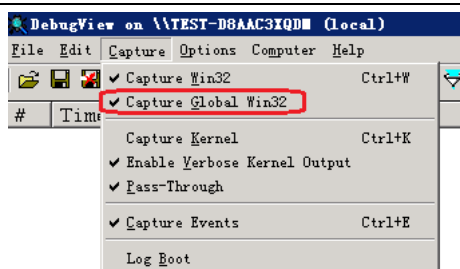
保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

三十、 POST 策略(POST 请求内容关键字过滤)

如果开启本策略,WAF 将对所有 POST 请求的内容进行关键字检查,如果发现非法关键字,就立即拦截请求.

为方便用户调试 POST 内容过滤关键字,WAF 对接收到的 POST 请求内容一律进行下列两种方式的输出操作:

1. WAF 检测服务器中是否存在调试器,如果存在,则把 POST 请求内容输出到调试器中.
 - 用户在服务器中可以用 **Dbgview** 工具([下载地址 1](#),[下载地址 2](#))查看到 WAF **实时输出**接收到的 POST 请求内容数据.注意,如果用户在远程桌面中运行 **Dbgview**,则必须勾选“Capture->Caputre Global Win32”方能接收到 WAF 的**实时输出**数据,如下图所示:



➤ **提示:**调试完毕后,用户应关闭 **Dbgview** 工具,以减轻 WAF 的工作量.

2. WAF 检测服务器 **C 盘**根目录下是否存在 **__skd_post_debug.txt** 文件,如果存在该文件,而且该文件 **users** 组用户具有写入权限,则把 POST 请求内容附加写入该文件中.

➤ 用户可以打开该文件查看 WAF 接收到的 POST 请求内容数据.

➤ **提示:**调试完毕后,用户应 重命名/删除 **C 盘**根目录下的 **__skd_post_debug.txt** 文件,以减轻 WAF 的工作量.

提示:用户可使用本策略拦截基于 POST 实施的 SQL 注入、XSS 等攻击.

用户可以设置**原始匹配关键字**(每个关键字最长 16 字节)和**正则表达式匹配关键字**(每个关键字最长 64 字节)这两种,且都不区分大小写,WAF 检测关键字时,将分别检测原始匹配的关键字和正则表达式匹配的关键字.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

三十一、 POST 策略(POST 请求 URL 限制)

如果开启本策略,WAF 将限制允许 POST 请求的 URL,未明确允许的 URL 将被禁止 POST 请求.

提示: 开启本策略可以用于阻止黑客登录一些 Webshell (网页后门),因为黑客登录 Webshell 时,一般都需要提交相关口令,提交相关口令通常都需要对

Webshell 页面进行 POST 请求方能完成.

例如,假设 index.asp 网页被黑客在某一时间植入了后门,并且网站管理员一直未发现该后门的存在,黑客经常对该页面进行 POST 请求来登录后门.现在用户开启了本策略,只设置了对 /login.asp 页面允许 POST 请求,其它页面不允许 POST 请求,则任何对 index.asp 的 POST 请求都将被 WAF 拦截,因而黑客再也无法登录该网页后门来危害网站.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

三十二、 COOKIE 策略(COOKIE 内容关键字过滤)

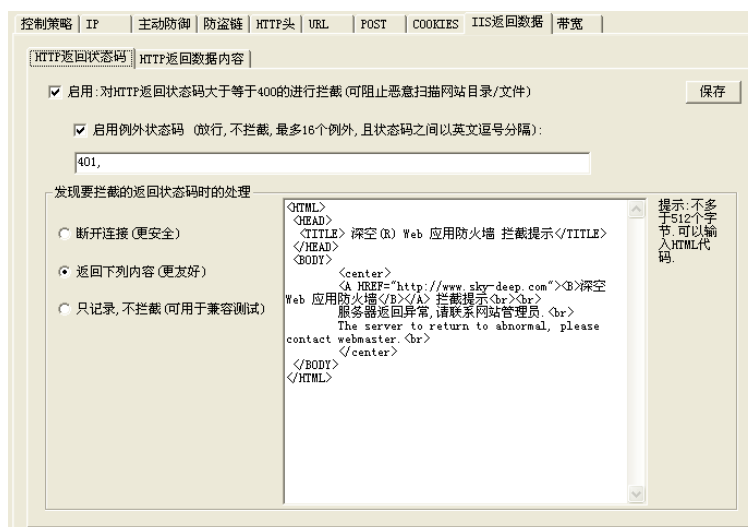
如果开启本策略,WAF 将对所有请求的 COOKIE 进行关键字检查,如果发现非法关键字,就立即拦截请求.

提示:用户可使用本策略拦截基于 COOKIE 实施的 SQL 注入攻击.

用户可以设置**原始匹配关键字**(每个关键字最长 16 字节)和**正则表达式匹配关键字**(每个关键字最长 64 字节)这两种,且都不区分大小写,WAF 检测关键字时,将分别检测原始匹配的关键字和正则表达式匹配的关键字.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

三十三、 IIS 返回数据策略(HTTP 返回状态码过滤)



如果开启本策略,WAF 将对所有 HTTP 返回状态码(流出 IIS 的数据)进行检查,对非例外的而且返回状态码大于等于 400 的都进行拦截。

黑客攻击时,经常会利用服务器的一些 400 及其以上的状态码来分析服务器漏洞(比如根据 web 服务器返回的 404 状态码来猜解 web 目录中敏感文件的路径),因此,WAF 拦截这些状态码并发送伪造后的欺骗性状态码,将能够极大地迷惑入侵者。

提示:用户可以设置一些例外状态码(要求 WAF 强制放行的状态码)。

根据 RFC2616,HTTP 返回状态码分类如下(详情请参考 RFC2616 文档)

- 1xx: 信息性——收到请求,继续处理
- 2xx: 成功性——成功收到、理解并接受行动
- 3xx: 重定向——必须采取进一步行动来完成请求
- 4xx: 客户端错误——请求包含错误语法或不能完成
- 5xx: 服务器错误——服务器没有成功完成显然有效的请求

具体如下:

1xx: 信息性——收到请求,继续处理

"100" : Continue

"101" : Switching Protocols

2xx: 成功性——成功收到、理解并接受行动

"200" : OK

"201" : Created

"202" : Accepted

"203" : Non-Authoritative Information

"204" : No Content

"205" : Reset Content

"206" : Partial Content

3xx: 重定向——必须采取进一步行动来完成请求

"300" : Multiple Choices

"301" : Moved Permanently

"302" : Found

"303" : See Other

"304" : Not Modified

"305" : Use Proxy

"307" : Temporary Redirect

4xx: 客户端错误——请求包含错误语法或不能完成

"400" : Bad Request

"401" : Unauthorized

"402" : Payment Required

"403" : Forbidden

"404" : Not Found

"405" : Method Not Allowed

"406" : Not Acceptable

"407" : Proxy Authentication Required

"408" : Request Time-out

"409" : Conflict

"410" : Gone

"411" : Length Required

"412" : Precondition Failed

"413" : Request Entity Too Large

"414" : Request-URI Too Large

"415" : Unsupported Media Type

"416" : Requested range not satisfiable

"417" : Expectation Failed

5xx: 服务器错误——服务器没有成功完成显然有效的请求

"500" : Internal Server Error

"501" : Not Implemented

"502" : Bad Gateway

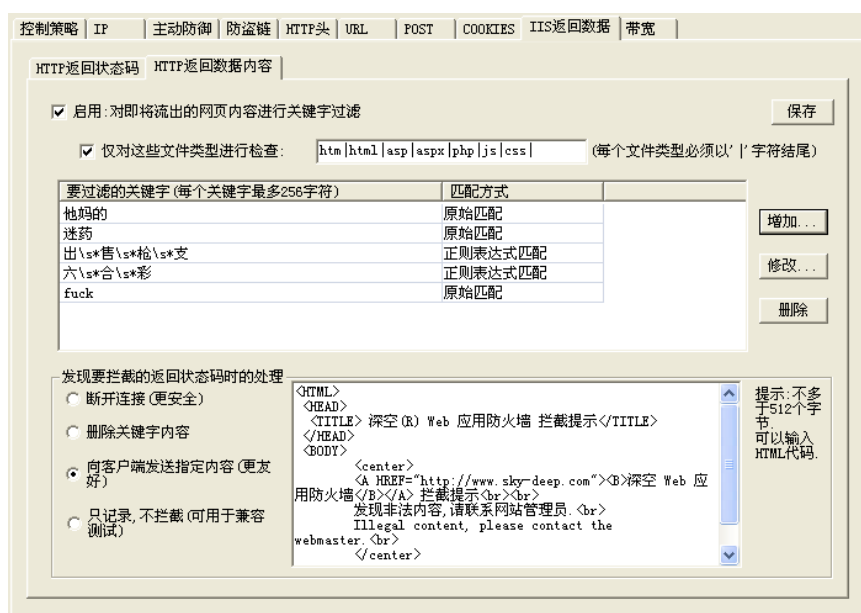
"503" : Service Unavailable

"504" : Gateway Time-out

"505" : HTTP Version not supported

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

三十四、 IIS 返回数据策略(HTTP 返回内容过滤/网页内容过滤)



如果开启本策略,WAF 将对所有 HTTP 返回内容(流出 IIS 的数据,即网页内容)进行关键字检查,用户可以设置当 WAF 在网页内容中发现非法关键字时采取的处理方式,目前有 4 种处理方式可供用户选择:

- 断开连接(更安全):** 立即断开连接.
- 删除关键字内容:** 只删除网页中的非法关键字内容,其它内容依然正常流出.注意:因为本处理方式需要查找与剔除非法关键字,所以会较慢.

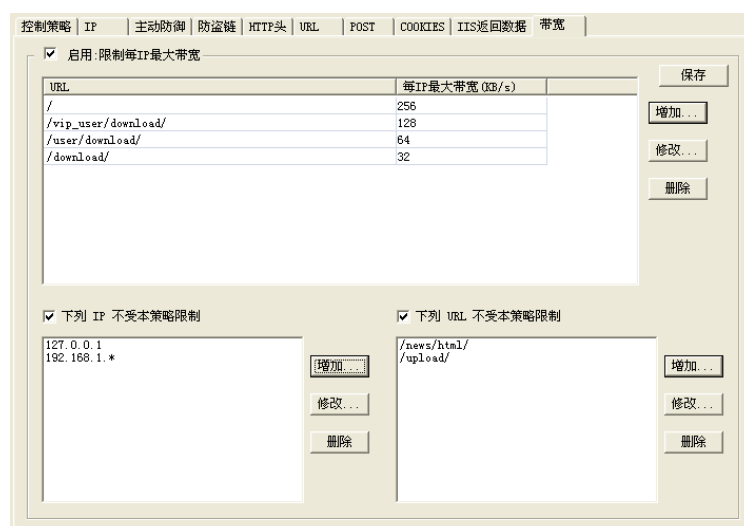
- c. **向浏览者发送指定信息:** 比如向浏览者发送“发现非法内容”等文字.
- d. **只记录,不拦截(可用于兼容测试):** WAF 记录下所有不合策略的请求但不拦截.本方式可以用来测试当前策略和网站的兼容程度,这期间网站的正常运行不受影响,用户可以逐步调试策略,直至满意为止.

用户可以设置**原始匹配关键字**(每个关键字最长 16 字节)和**正则表达式匹配关键字**(每个关键字最长 64 字节)这两种,且都不区分大小写,WAF 检测关键字时,将分别检测原始匹配的关键字和正则表达式匹配的关键字.

提示:推荐用户只对指定类型的网页(如:htm、html、asp、aspx、php、js、css)进行网页内容检查,这样可以让 WAF 减少不必要的网页内容过滤开销,否则 WAF 将对所有流出数据都进行过滤而不管当前数据是什么文件类型.

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

三十五、 带宽策略



如果开启本策略,WAF 将对指定的 URL 及其子 URL(子目录)进行带宽限制,除了例外 URL 和例外 IP,其它 IP 的最大访问/下载带宽都将被限制到用户设置的

最大带宽以内.

本策略的启用可以防止因为个别 IP 占据大量带宽导致的影响正常用户访问/下载.

提示:本产品中计算带宽的方式包括了 HTTP 的头部等信息,比通常意义的带宽大 2.5 倍左右(这一数值仅仅过初步测试,未经严格的测试,用户应根据实际情况进行调整).例如,假设用户希望对/download/目录限制每个 IP 最大下载带宽为 128kb/s,则用户应设置最大限制带宽为 $128 \times 2.5 = 320 \text{kb/s}$.

用户可以设置一些不受带宽限制的 IP/IP 段.

用户可以设置一些不受带宽限制的 URL 及其子 URL(子目录).

保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方能生效.

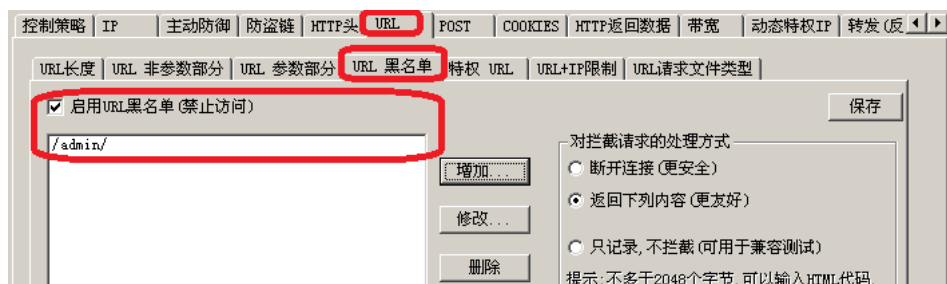
三十六、 动态特权 IP 策略

动态特权 IP 策略提供一种功能 :使合法用户能够临时不受 WAF 的各种策略限制,如直接查看到服务器原始返回信息、不受限制地访问黑名单 URL 等.

例如：用户可以将网站后台路径列入黑名单,同时开启**动态特权 IP** 策略,设置一个隐蔽的进入动态特权 IP 列表的 URL,平时后台路径处于黑名单 URL 列表,因此黑客无法访问,合法用户要访问后台时,只需访问一次进入动态特权 IP 列表的 URL,然后就可以不受限制地访问到后台路径.下面举例说明：

假设用户网站后台路径是:www.test.com/admin/login.asp

现在WAF的**URL->URL黑名单**策略中,将 /admin/列入了黑名单,如下图所示：

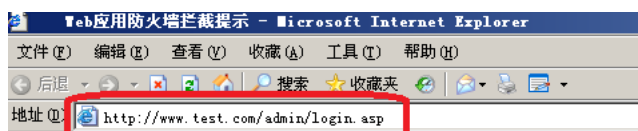


同时,开启了WAF的动态特权IP策略,设置/zhimakaimen.kaimen为进入动态特权 IP 列表的 URL,如下图所示：



配置保存后,点击“控制策略” -> “立即加载最新配置”,使策略生效.

在未访问进入动态特权 IP 的 URL 之前,访问网站后台:
www.test.com/admin/login.asp 将被拦截,并可看到类似如下页面:



Web应用防火墙->拦截请求

提示: 用户可自定义该拦截页面

出现该页面的原因:

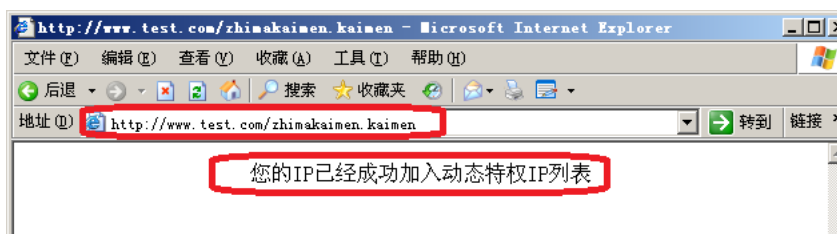
1. 该路径不允许访问:

(“日志”->“拦截日志”中记录了具体信息)

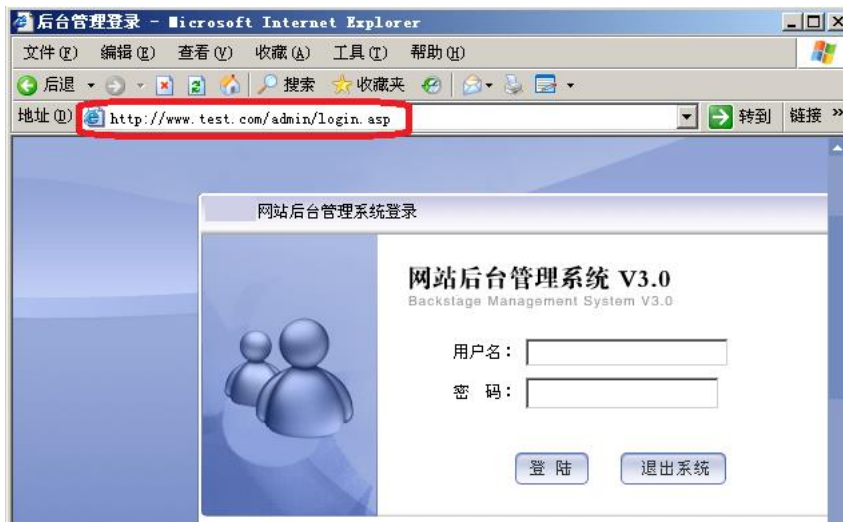
策略位置: “URL”->“URL黑名单”

技术支持:

用户再访问进入动态特权 IP 的 URL,WAF 将把用户的 IP 加入动态特权 IP 列表,并可以看到如下页面:



随后再次访问网站后台: www.test.com/admin/login.asp 即可正常看到后台登录页面:



完毕.

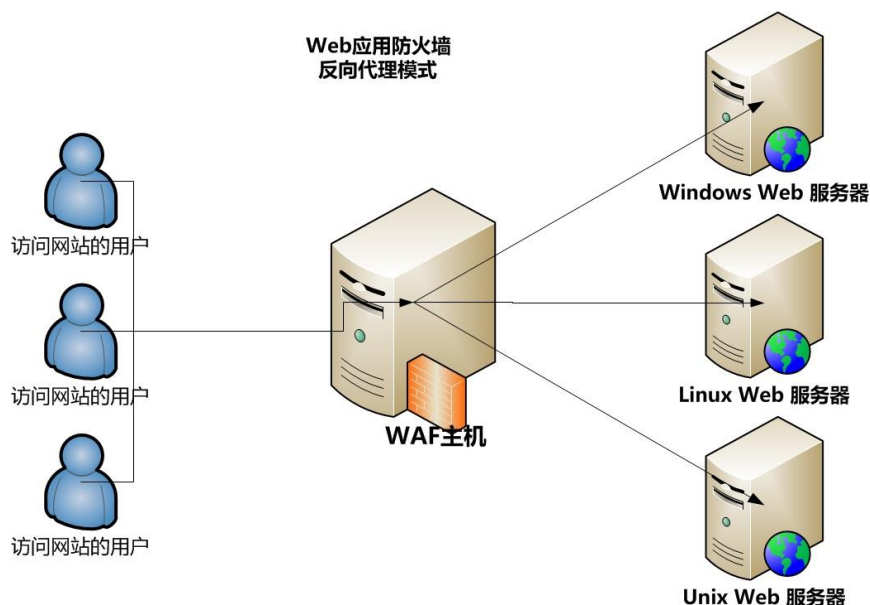
保存本策略配置后,点击“控制策略” -> “立即加载最新配置” 后方可生效.

第七章 制作硬件 WAF

通过开启 WAF 的**转发(反向代理)**策略,可以将 WAF 所处的服务器主机变成一台专职的硬件 web 应用防火墙(以下简称**硬件 WAF**).

The screenshot shows the configuration window for the '转发(反向代理)' (Forward (Reverse Proxy)) strategy. The window has a tabbed interface at the top with the following tabs: 控制策略, IP, 主动防御, 防盗链, HTTP头, URL, POST, COOKIES, HTTP返回数据, 带宽, and 转发(反向代理). The '转发(反向代理)' tab is selected. Inside the window, there is a checkbox labeled '启用转发(反向代理)' which is checked. To the right of this checkbox is a '保存' (Save) button. Below the checkbox, there are two input fields: '转发到IP:' with the value '127.0.0.1' and '端口:' with the value '81'. Below these fields is a section titled '以下配置如果不熟悉请保持默认' (If you are not familiar with the following configuration, please keep the defaults). This section contains three checkboxes, all of which are unchecked: '自定义URL参数部分代码页', '自定义转发超时设置', and '自定义转发接收超时设置'. To the right of these checkboxes is a '恢复默认' (Restore Defaults) button. Below the checkboxes, there are three input fields for timeout settings: '转发连接超时(毫秒)' with the value '60000', '转发发送超时(毫秒)' with the value '30000', and '转发接收超时(毫秒)' with the value '30000'.

如开启**转发(反向代理)**策略,WAF 将把清洗后的请求转发给指定 IP 的指定端口,并把返回数据经清洗后回传给请求者.用户可以通过开启该策略实现对非 windows 系统的 web 应用安全防护,如下图所示:



一、 硬件准备

一台可安装 windows 服务器操作系统的 PC 机或服务器,当作 WAF 的硬件.

- **处理器**：至少 Intel Pentium III,推荐双核以上的多核多线程 CPU.
- **内存**：至少 256MB,推荐 2G 以上.
- **硬盘**：至少剩余空间在 10G 以上 ,推荐剩余空间 15G 以上.

二、 软件准备

- **Windows 服务器操作系统一套,如:**

Windows Server 2003 Enterprise Edition SP2

Windows Server 2008 Enterprise Edition SP2/R2

Windows Server 2012 Enterprise Edition

- **深空 web 应用防火墙系统软件一套.**

三、 部署方式

以下步骤描述基于假设:

网关:

192.168.1.1

硬件 WAF (Windows 服务器操作系统):

192.168.1.2

web 服务器(Linux 操作系统)IP:

192.168.1.3,HTTP 服务端口:80

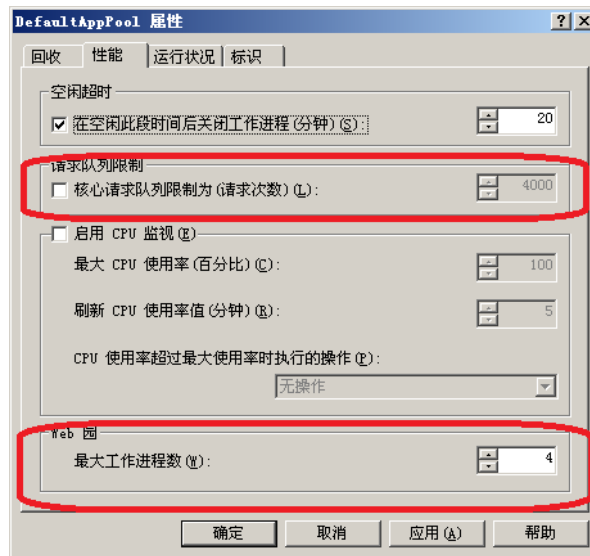
要求:

在 192.168.1.2 上部署 WAF,从而把 192.168.1.2 改造成一台硬件 WAF,然后用它保护 192.168.1.3 这个 Linux 操作系统 web 服务器的 HTTP(80 端口)web 服务.

下面是操作步骤:

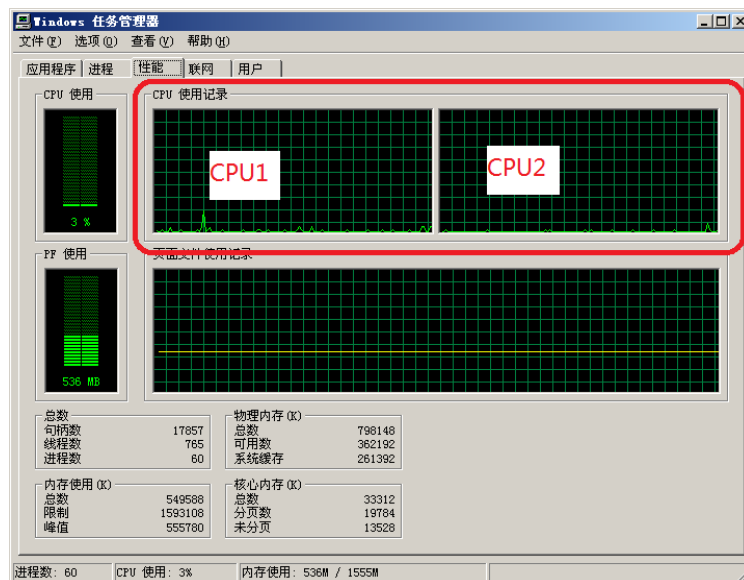
❖ **第一步:** 在硬件主机(192.168.1.2)上安装好 windows 服务器操作系统,并安装好 IIS(如果是 64 位系统或者 IIS7.0 以后版本,请参阅[注意事项](#)),然后按下面的说明调整默认应用程序池属性配置:

1. 取消请求队列限制,如下图所示;

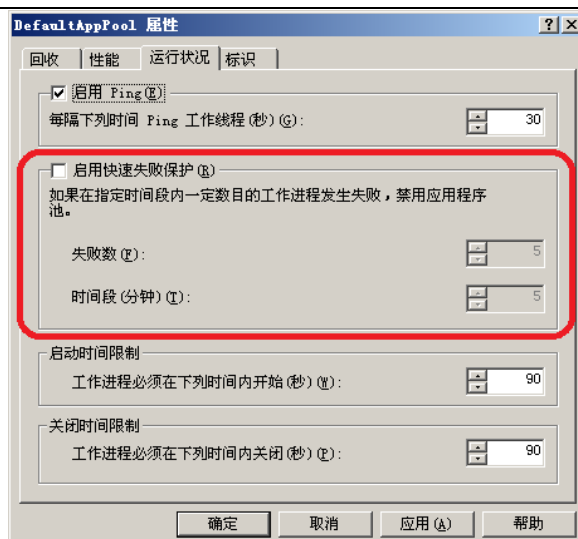


2. 设置 web 园最大工作进程数: 设置为任务管理器所见 CPU 个数的 2 倍或 4 倍,如上图所示.

下图任务管理器所示 CPU 个数为 2,则最大工作进程数设置为 4 或 8 (注意 :为增强并发性,无论 CPU 个数为多少,此值都不得小于 4).



3. 关闭快速失败保护,如下图所示 :



4. 完毕,点击“确定”保存.

❖ **第二步:**在硬件主机(192.168.1.2)上,把下面的内容另存为 reg 文件,也就是注册表文件,然后双击导入:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"TcpMaxHalfOpen"=dword:000001f4
"SynAttackProtect"=dword:00000001
"TcpMaxHalfOpenRetried"=dword:00000190
"EnablePMTUDiscovery"=dword:00000000
"TcpMaxPortsExhausted"=dword:00000005
"KeepAliveTime"=dword:00000bb8
"KeepAliveInterval"=dword:000003e8
"TcpMaxDataRetransmissions"=dword:00000002
"NoNameReleaseOnDemand"=dword:00000001
"DefaultTTL"=dword:00000040
"TcpTimedWaitDelay"=dword:00000005
"TcpNumConnections"=dword:00ffffff
"MaxUserPort"=dword:0000fffe
"MaxHashTableSize"=dword:00010000
"MaxFreeTcbs"=dword:ffffff
```

注意:导入完成后,必须重新启动操作系统.

❖ **第三步:** 在硬件主机(192.168.1.2)上安装深空 web 应用防火墙系统软件,并开启转发(反向代理)策略.转发 IP: 192.168.3 ,转发端口: 80,保

存配置,并立即加载最新配置.如下图所示:

控制策略 | IP | 主动防御 | 防盗链 | HTTP头 | URL | POST | COOKIES | HTTP返回数据 | 带宽 | 转发(反向代理)

☒ 启用转发(反向代理)

转发到IP: 192.168.1.3

端口: 80

以下配置如果不熟悉请保持默认

☐ 自定义URL参数部分代码页 936

☐ 自定义转发超时设置

转发连接超时(毫秒) 60000

转发发送超时(毫秒) 30000

转发接收超时(毫秒) 30000

保存

恢复默认

- ❖ **第四步:** 在网关处,将原来发往 192.168.1.3 的 80 端口数据改成发往硬件 WAF 的 IP 192.168.1.2 的 80 端口.
- ❖ **第五步:搭建完毕.**此时 192.168.1.2 已经可以对 192.168.1.3 进行 web 应用防护.

四、 其它选项说明

➤ 自定义 URL 参数部分代码页

WAF 默认配置 URL 参数部分代码页: **65001**(也就是 UTF8).

WAF 所转发的 URL 参数部分中,如果含有跟编码有关联的信息(比如 URL 参数部分出现了中文文字),而且该信息不是 UTF8 编码的,则用户必须在此调整代码页.全球各语系编码代码页列表可参考:

[http://msdn.microsoft.com/en-us/library/dd317756\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/dd317756(VS.85).aspx)

下图所示为修改 URL 参数部分代码页为 **936**(GB2312 编码).

控制策略 | IP | 主动防御 | 防盗链 | HTTP头 | URL | POST | COOKIES | HTTP返回数据 | 带宽 | 转发(反向代理)

☒ 启用转发(反向代理) 保存

转发到IP: 192.168.1.3

端口: 80

以下配置如果不熟悉请保持默认

☒ 自定义URL参数部分代码页 936 恢复默认

☐ 自定义转发超时设置

转发连接超时(毫秒) 60000

转发发送超时(毫秒) 30000

转发接收超时(毫秒) 30000

➤ 自定义转发超时设置

转发请求时,涉及到连接、发送、接收超时时间设置,用户可以在此调整 WAF 默认超时时间.

默认连接超时: 60000 毫秒(60 秒).

默认发送超时: 30000 毫秒(30 秒).

默认接收超时: 30000 毫秒(30 秒).

控制策略 | IP | 主动防御 | 防盗链 | HTTP头 | URL | POST | COOKIES | HTTP返回数据 | 带宽 | 转发(反向代理)

☒ 启用转发(反向代理) 保存

转发到IP: 192.168.1.3

端口: 80

以下配置如果不熟悉请保持默认

☒ 自定义URL参数部分代码页 936 恢复默认

☒ 自定义转发超时设置

转发连接超时(毫秒) 60000

转发发送超时(毫秒) 30000

转发接收超时(毫秒) 30000

提示：保存本策略配置后,点击“控制策略”->“立即加载最新配置”后方可生效.

第八章 日志类操作

本产品中的日志分为 **WAF 拦截日志**、**管理日志**、**错误日志**和**产品日志**这四种.

其中,产品日志只有 **产品管理员用户** 使用 **管理员客户端** 方能查看.

其中,对 WAF 拦截日志,用户可以控制日志记录的对象,即要求 WAF 哪些拦截日志要记录,哪些拦截日志不要记录.

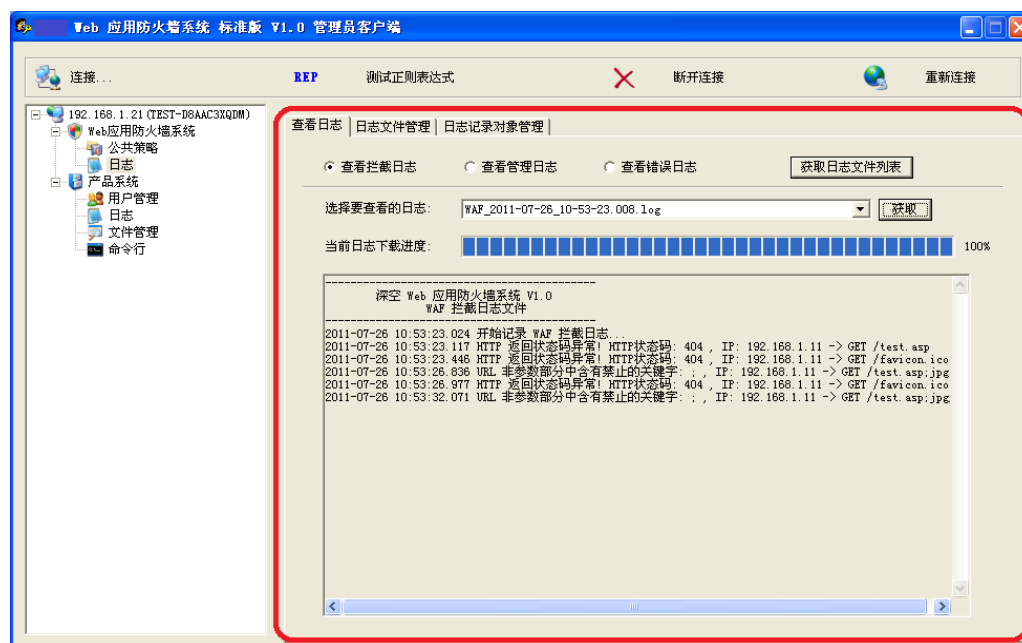
WAF 拦截日志: 记录了 WAF 拦截的每一条请求的详细信息,包括: 拦截时间(精确到毫秒)、拦截的原因、关键字(如果有)、源 IP 地址、请求方式、请求的 URL 等信息.

管理日志: 记录了策略执行和用户的对策略的修改操作信息,包括: 当前策略对应用户的登录/退出的时间(精确到毫秒)、修改时间(精确到毫秒)、执行修改操作的用户名、修改的内容等信息.

错误日志: 记录了当前策略的在任一过程中发生的错误信息.

产品日志: 记录了产品运行和管理员修改产品相关配置的信息,包括: 产品进程的启动时间、结束时间、退出时间、退出的原因、管理员/普通用户的登录时间、管理员/普通用户的退出时间、各个策略的加载情况、私有策略的创建/删除情况等信息.

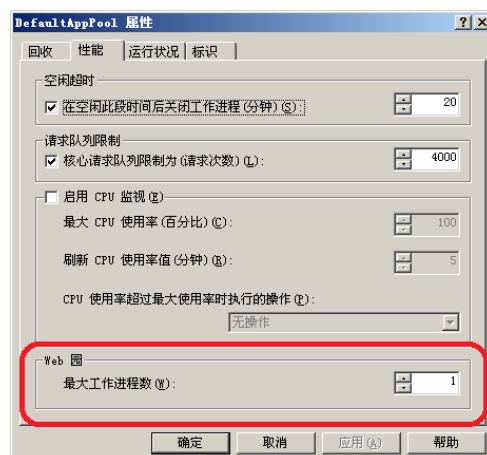
一、 查看日志文件内容



如上图所示,用户可以通过“**查看日志**”来查看各种日志文件的内容。

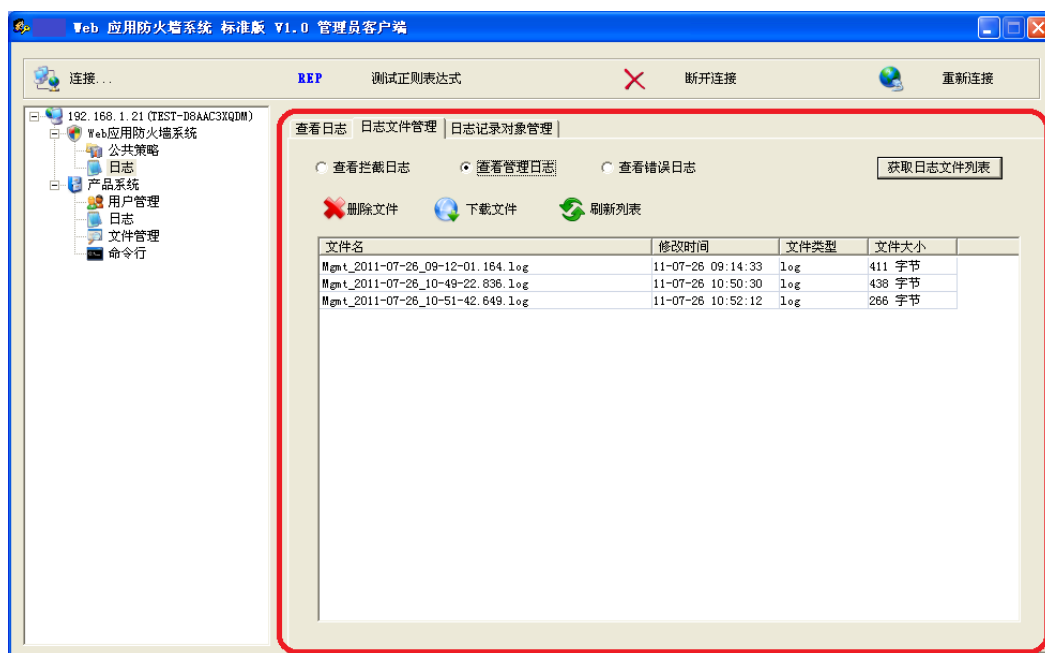
提示:用户需点击“获取日志文件列表”后,才能列出当前的日志文件列表。

提示:因为本产品设计成一个 IIS 工作进程(如 w3wp.exe)对应一个 WAF 拦截日志文件,所以在默认情形下,1 个网站对应的最新 WAF 拦截日志只有 1 个。对 IIS 的 6.0 及以后版本,如果某网站所在**应用程序池**的 Web 园设置的“最大工作进程数”大于 1 个,则该网站对应的最新 WAF 拦截日志文件也将可能大于 1 个。



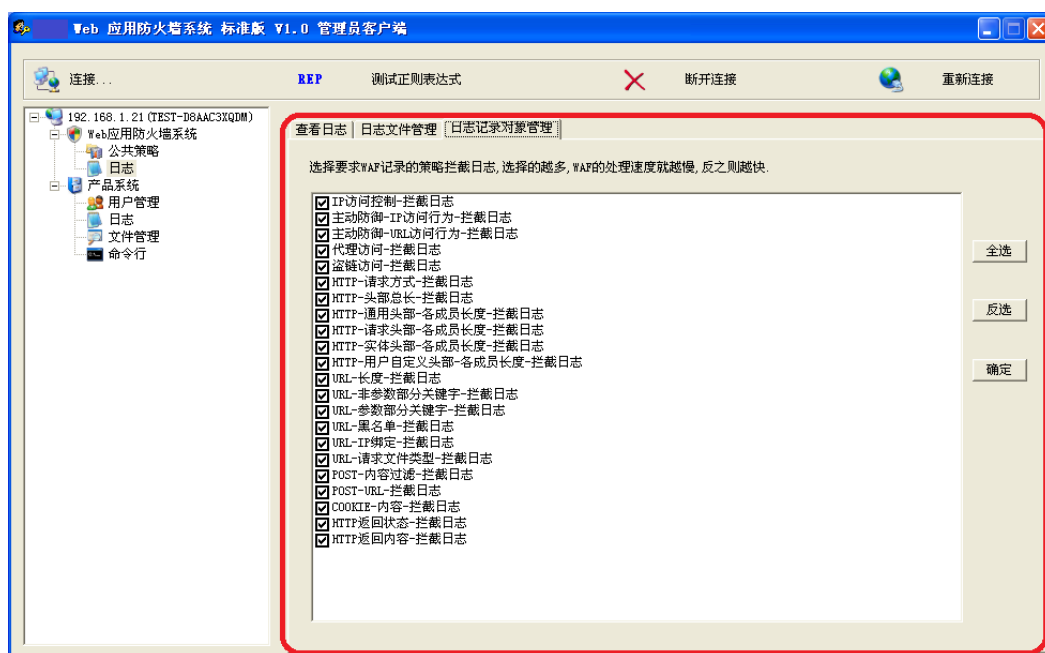
提示:在日志显示区,客户端会每隔 5 秒自动刷新一次日志。

二、 日志文件管理



如上图所示,用户可以通过“**日志文件管理**”来查看、删除（可批量删除）下载（可批量下载）各种日志文件。

三、 日志记录对象管理



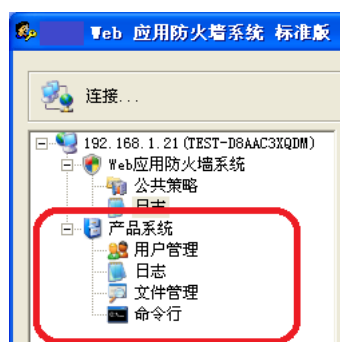
如上图所示,用户可以通过“**日志记录对象管理**”来选择需要日志记录的对象,

用户可以控制日志记录的对象,即要求 WAF 哪些拦截日志要记录,哪些拦截日志不需要记录.

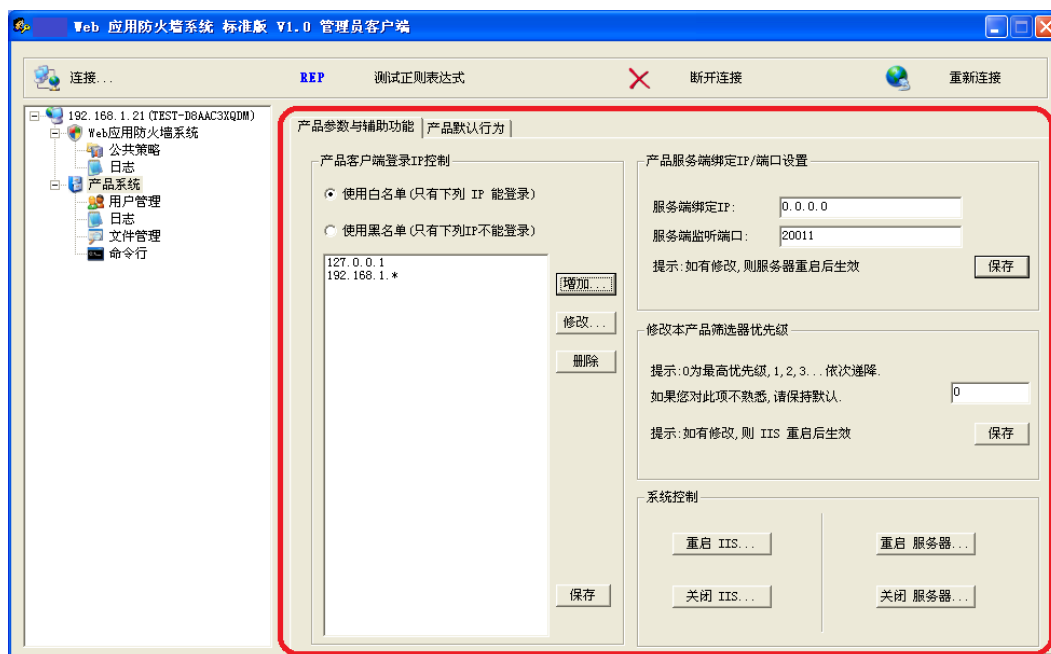
提示:用户可以根据自身情况选择需要日志记录的对象,原则上应尽量少选,因为需要日志记录的对象越多,WAF 的速度就越慢.

第九章 产品系统操作

如下图所示,左边树形列表中的 " 产品系统 ",该系统只有 **产品管理员用户** 使用 **管理员客户端** 才能查看.



一、产品客户端登录 IP 限制



如上图所示,用户可以对产品客户端的登录 IP 进行限制,以增强产品的安全性.

本产品提供了黑名单 IP 和白名单 IP 这两种策略来限制客户端的登录范围.

使用黑名单 IP 时,只有黑名单中的 IP 不可登录;使用白名单 IP 时,只有白名单中的 IP 才允许登录,其它一律禁止登录。

用户可以设置一个或多个 IP/IP 段为黑名单或白名单。

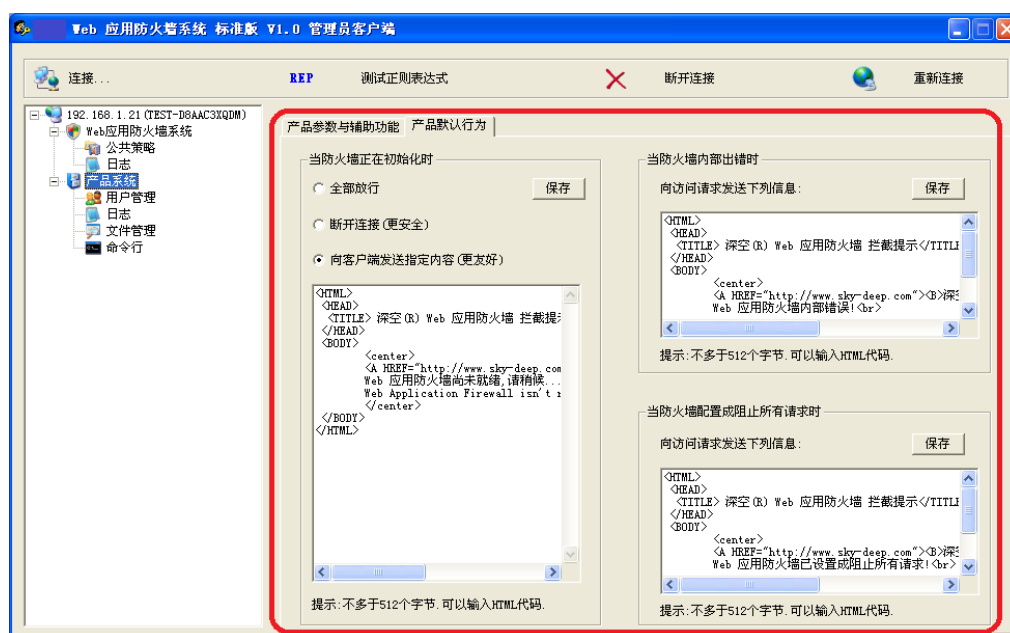
二、 产品服务端绑定 IP/端口

产品默认在所有网卡上监听 20011 端口,用户可以根据自身的情形进行修改绑定 IP 或监听的端口。

三、 系统控制

本产品的**管理员客户端**提供了对操作系统的一些快捷控制按钮,包括“重启 IIS”、“关闭 IIS”、“重启服务器”、“关闭服务器”。

四、 产品默认行为



如上图所示,用户可以对“当防火墙正在初始化时”、“当防火墙内部出错时”、

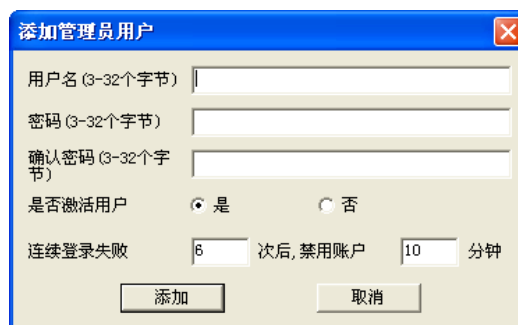
“当防火墙配置成阻止所有请求时”这三种情况向浏览者发送的信息作出自定义。

特别地,对“当防火墙正在初始化时”这种情形,用户可以设置 WAF 的处理方式为下列之一:

- a. **全部放行:** 策略初始化完成前,放行所有请求.
- b. **断开连接(更安全):** 立即断开连接.
- c. **向浏览者发送指定信息:** 如向浏览者发送“WAF 正在初始化,请稍候再刷新...”。

五、 用户管理

在“用户管理”中,管理员用户可以重设自己的用户名和密码,也可以添加、删除、修改一个管理员/普通用户等,如下图所示添加管理员用户:



该对话框用于添加新的管理员用户。它包含以下字段和选项：

- 用户名 (3-32个字节): 文本输入框
- 密码 (3-32个字节): 文本输入框
- 确认密码 (3-32个字节): 文本输入框
- 是否激活用户: 单选按钮，默认选中“是”，另一个选项为“否”。
- 连续登录失败: 数字输入框，默认为 6。
- 次后, 禁用账户: 数字输入框，默认为 10。
- 分钟: 文本输入框，默认为 分钟。
- 底部有两个按钮: “添加”和“取消”。

管理员用户可以设置一个用户最多可连续登录失败的次数,以及超出此次时临时禁用该用户的分钟数.例如,产品默认对一个连续登录失败 6 次的用户会临时禁用其 10 分钟,在禁用时间内,此用户将被拒绝登录,即使输入正确的用户名和密码。

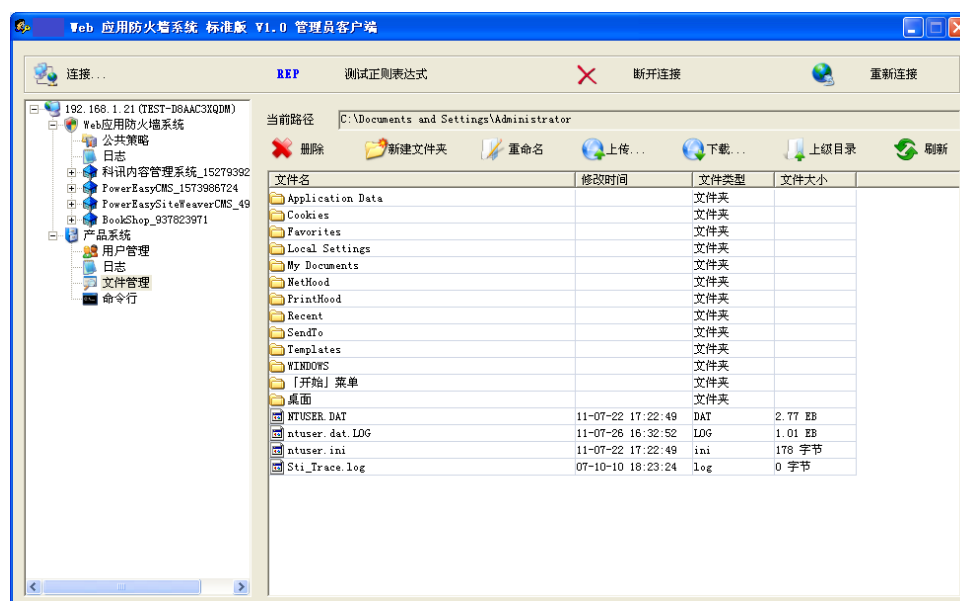
提示,在达到最多允许的连续登录失败次数之前,如果有一次成功登录,则该用户可连续登录失败的次数又将恢复成管理员用户指定的次数(默认为 6 次)。

在创建普通用户时,管理员用户可以给普通用户设置相关的权限,也就是该普通用户能够管理的站点(私有策略).如下图所示:



普通用户使用普通用户客户端登录时,只能看到它有权管理的站点(私有策略),并且不具备“产品系统”.本产品的普通用户这一概念方便 IDC 用户开设 Web 防火墙网络安全增值服务.

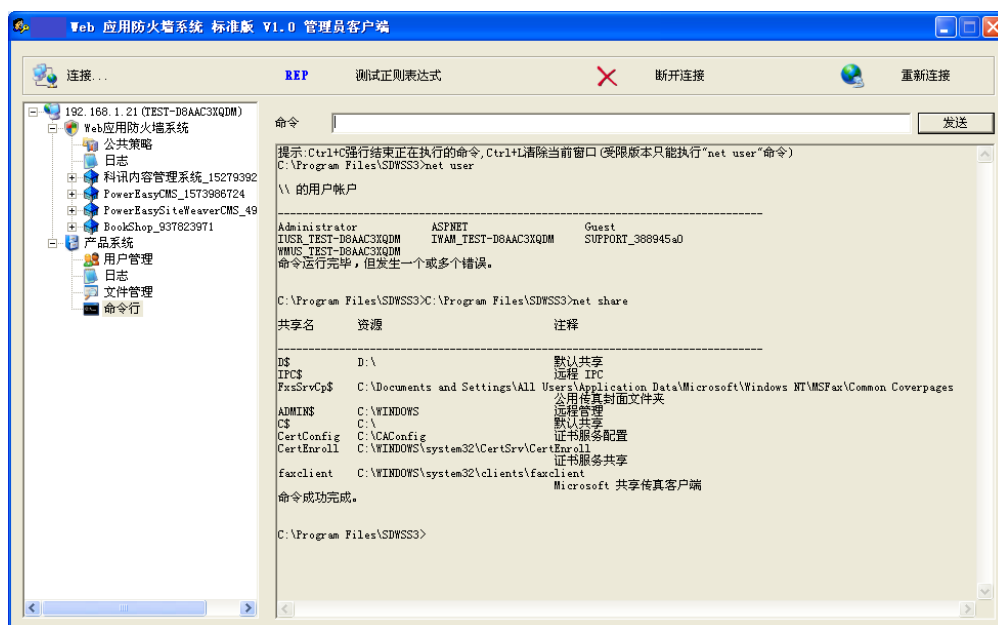
六、 文件管理



如上图所示,在“文件管理”中,用户可以对服务器中各个硬盘分区上的文件

进行管理,包括：删除、新建文件夹、重命名、上传文件/文件夹（含批量操作）、下载文件/文件夹（含批量操作）、刷新等。

七、 命令行



如上图所示,在“命令行”中,用户可以远程模拟执行 cmd 命令,如 net user、net share、tasklist、ping 等。

第十章 不同环境下的注意事项

若本产品即将安装在 64 位操作系统上,或者即将安装在 IIS7.0 及其以后版本的服务器中时,在安装产品前,须进行如下所述的额外配置.

若本产品安装在域控制器 (Domain Controller) 上,[请跳到这里](#) .

一、 Windows XP x64 / Windows Server 2003 x64 操作系统

1.打开 cmd.exe,切换到 inetpub 目录,在命令行中依次输入如下两行命令:

命令一:

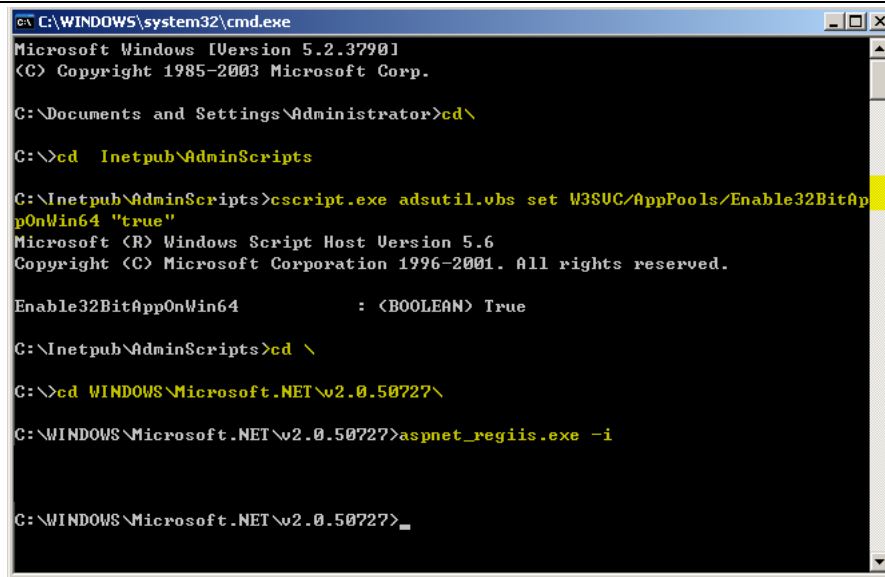
```
cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitAppOnWin64 "true"
```

命令二:

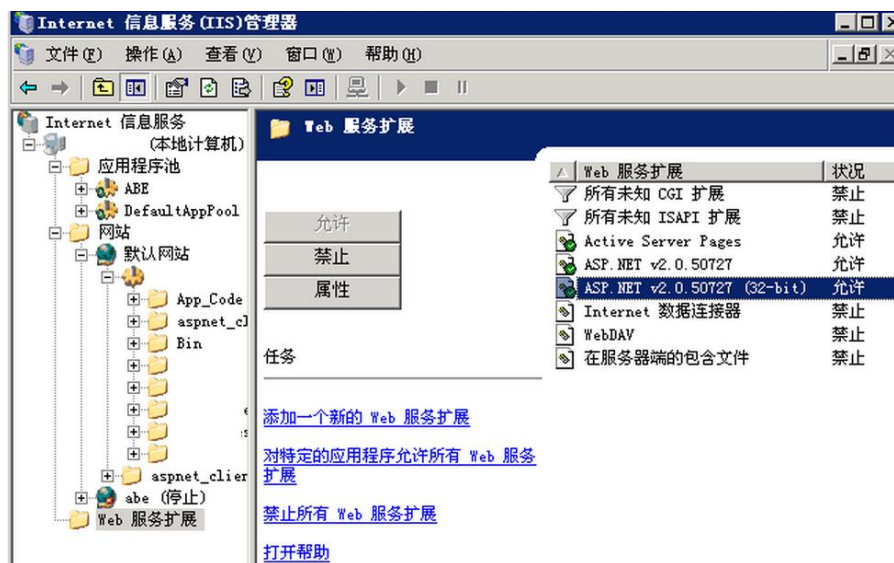
```
%SYSTEMROOT%\Microsoft.NET\Framework\<version>\aspnet_regiis.exe -i
```

(注意: "%SYSTEMROOT%" 是系统目录,一般是 c:\windows " <version>" 是 asp.net 版本号,视自身网站所运行的.net 版本而定)

如下图所示:



2. 设置 ASP.NET 32 位的 web 服务拓展为允许,如下图所示:



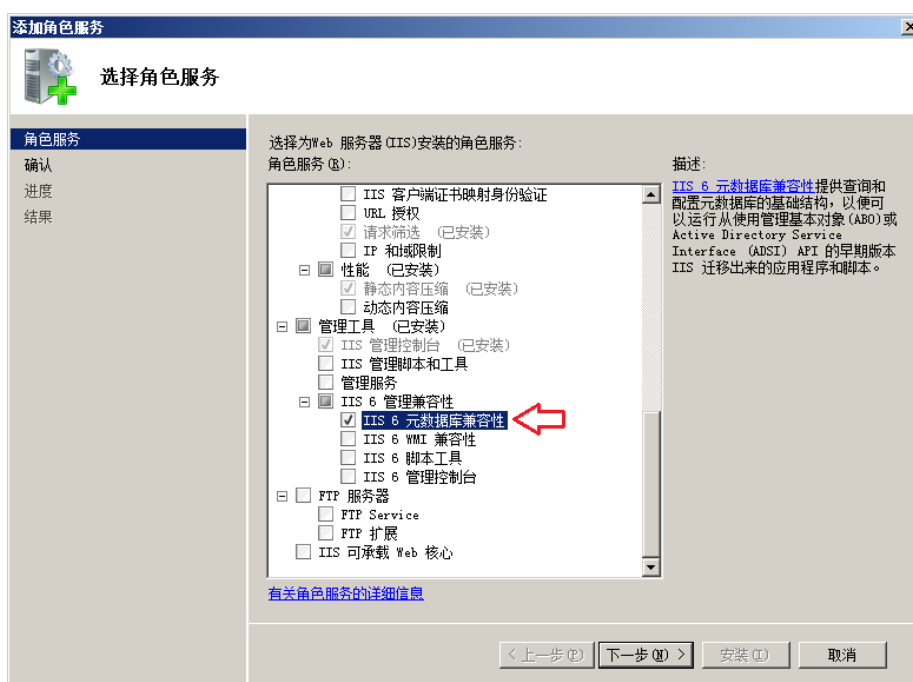
完成配置.

二、 IIS7.0 及其以后版本的环境中

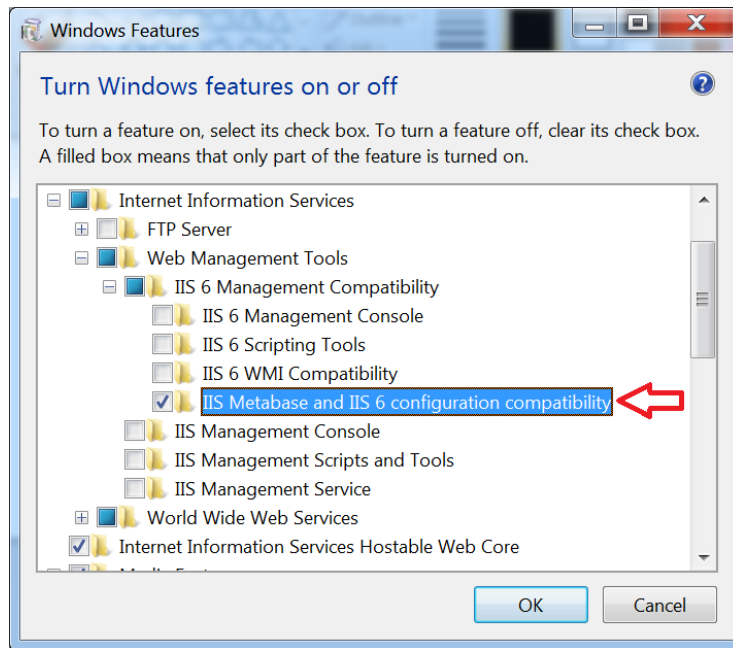
在 IIS7.0 及其以后版本的环境中安装本产品时,"IIS6 元数据库兼容性"角色必须确保已安装,否则在安装时会提示未安装 IIS.

提示 : 用户可以先尝试安装, 如果程序提示未安装 IIS, 再按下述步骤进行操作.

下图为 Windows Serve 2008 R2 控制面板->系统和安全->管理工具->服务器管理->“添加角色服务”的截图, 红色箭头所示的“IIS6 元数据库兼容性”必须勾选并安装.



下图为 Windows 7 控制面板->程序->“打开/关闭 Windows 角色”的截图, 红色箭头所示的“IIS 元数据库与 IIS6 配置兼容性”必须勾选并安装.



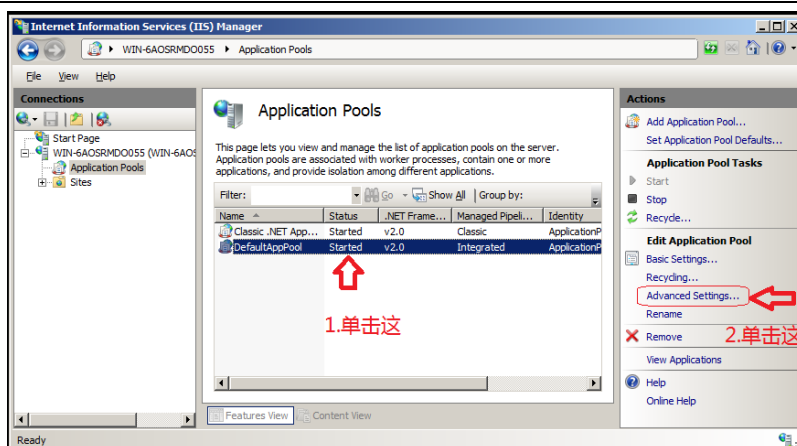
三、 Windows Vista x64 / Windows Server 2008 x64 / Windows 7 x64 / Windows Server 2012 / Windows 8 x64 操作系统

在 64 位操作系统中运行时,应用程序池必须设置成 32 位应用程序兼容模式:
应用程序的“高级设置”属性中,把“启用 32 位应用程序”设置成 TRUE.

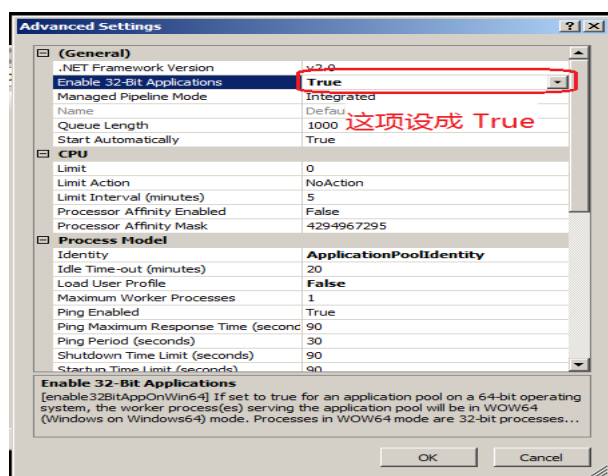
注意：下面的操作建立在假设被保护网站的应用程序池是默认的应用程序池 (DefaultAppPool)的基础上.如果被保护网站的应用程序池不是默认的应用程序池,请根据后面的示例,对相应的应用程序池进行配置.

1.打开 IIS 管理工具

2.按下图所示操作



3.弹出类似下图方框,按图中所示操作,随后单击"OK"关闭对话框,完成配置.



四、域控制器 (Domain Controller) 上的额外操作

如果本产品安装在域环境的域控制器(Domain Controller)上,则要检测 IIS 中的应用程序池标识(默认为 NETWORK_SERVICE 账户)是否是 IIS_WPG(Windows Server 2003)/IIS_IUSRS(Windows Vista 及以后) 组的成员.检测方法如下:

打开 cmd.exe,输入下面的命令:

对 Windows Server 2003 系统,执行下面的命令:

```
Net localgroup IIS_WPG
```

对 Windows Vista 及以后的系统,执行下面的命令:

```
Net localgroup IIS_IUSRS
```

查看执行结果中是否有应用程序池标识账户,如果应用程序池标识为上述组的成员,则下面操作可跳过.

否则,新创建一个账户,并把它加入到上述组中(Windows Server 2003 下加入 IIS_WPG 组,Windows Vista 及以后则加入 IIS_IUSRS 组).假设新创建账户的账户名为 AppPoolUser,则操作方法示例如下:

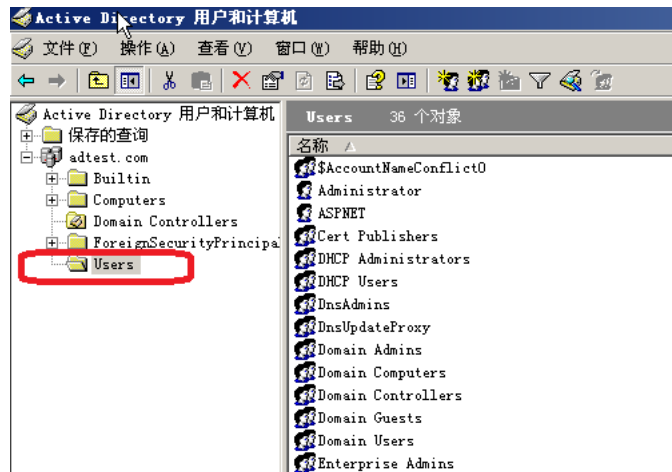
1. 首先打开 cmd.exe,输入并执行下面的命令:

```
Net user AppPoolUser Password123 /add
```

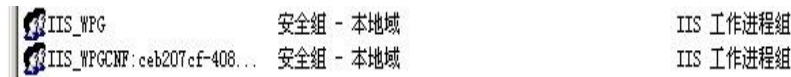
2. 然后按如下所述操作:

首先打开**控制面板->管理工具->Active Directory 用户和计算机**

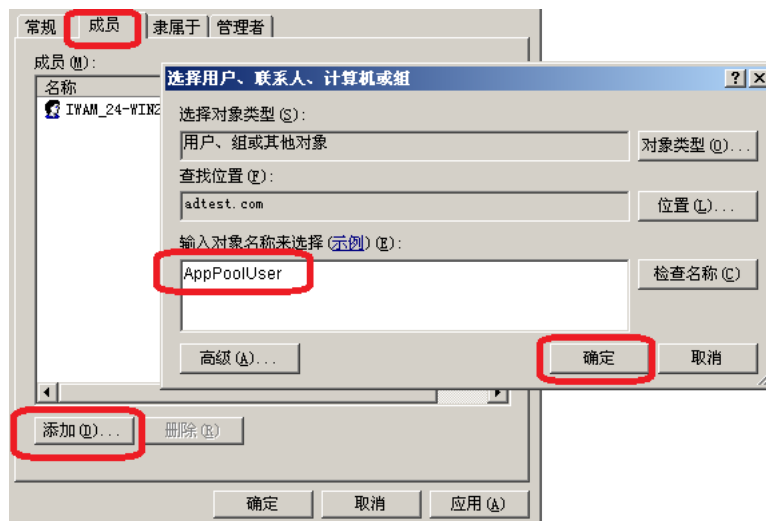
->Users



查看是否有类似 IIS_WPGCNF:xxxxxxx-....的 IIS 工作进程组,如下图所示:



如果有,则双击这个 IIS_WPGCNF:xxxxxxx-....用户组,选“成员”选项卡,然后把 AppPoolUser 用户加进去,如下图所示:



然后点击“确定”保存并关闭对话框。

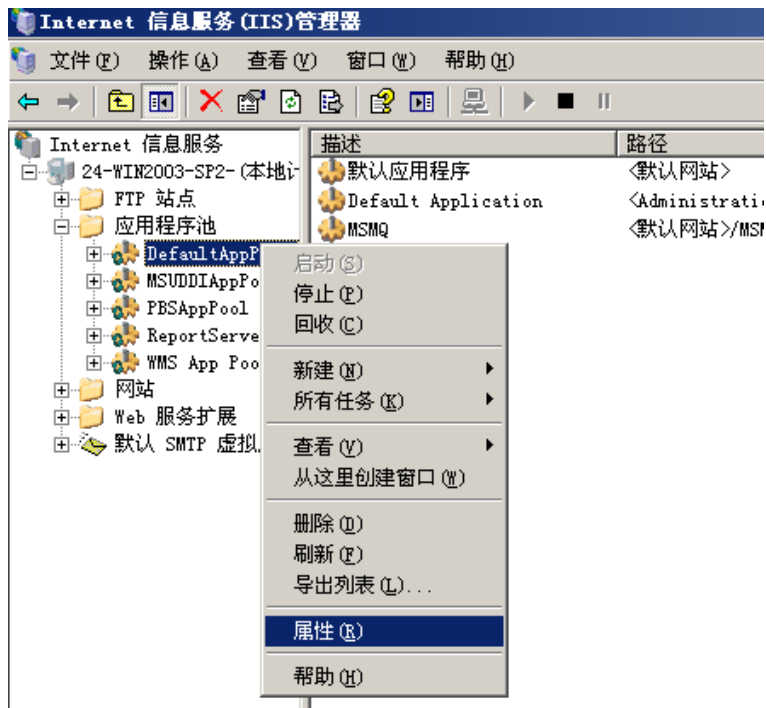
对 Windows Server 2003 系统,再执行下面的命令:

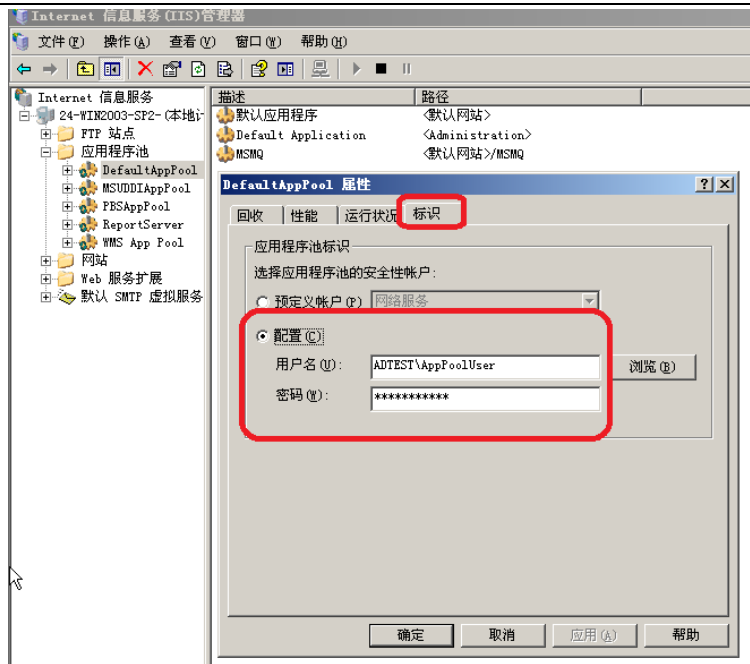
```
Net localgroup IIS_WPG AppPoolUser /add
```

对 Windows Vista 及以后的系统,再执行下面的命令:

```
Net localgroup IIS_IUSRS AppPoolUser /add
```

3. 再把应用程序池的标识改成 AppPoolUser ,如下图所示(Windows Server 2003 中的操作截图):





4. 最后重启 IIS(命令行下输入 iisreset).

5. 完毕.

第十一章 使用审计策略

本产品对自身安装目录下的所有文件都提供了对象访问审计策略支持.该项功能需要操作系统启用对象访问**审计策略**的配合,用户可根据自身安全要求决定是否启用该策略.

该功能简介:非管理员组 (administrators) 用户访问产品安装目录下的文件,都将失败,且该行为会被记录到操作系统安全日志中.

一、 启用对象访问审计策略

默认下,操作系统不打开该项审计,要启用该项审计,按如下方式操作:

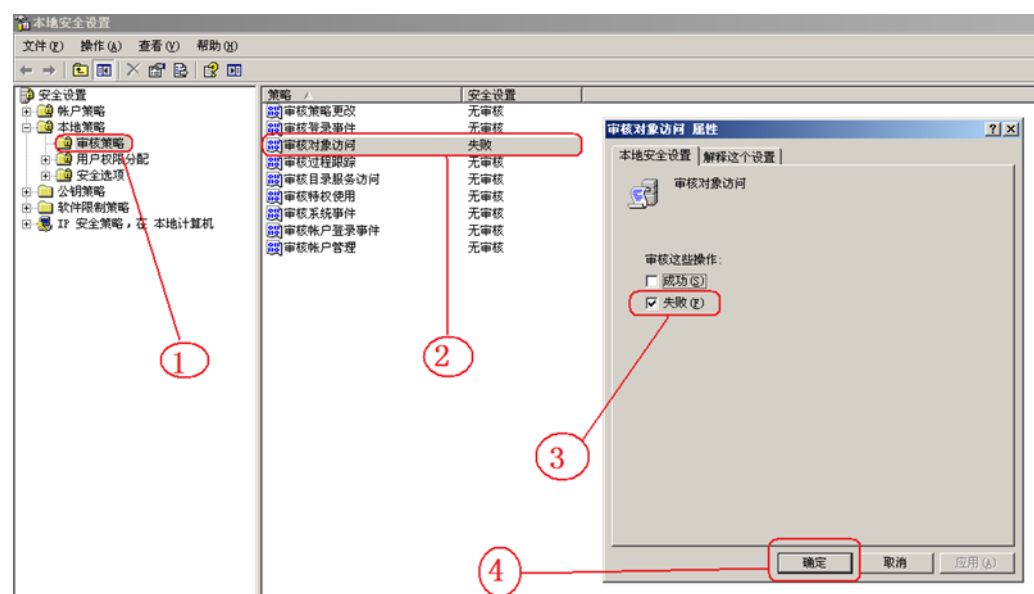
1:依次打开 " 控制面板 " -> " 管理工具 " -> " 本地安全策略 " -> " 本地策略 " -> " 审核策略 " ;

2:双击 " 审核对象访问 " ;

3:弹出的对话框中,单选 " 失败 (F) " 这项 ;

4:确定 ;

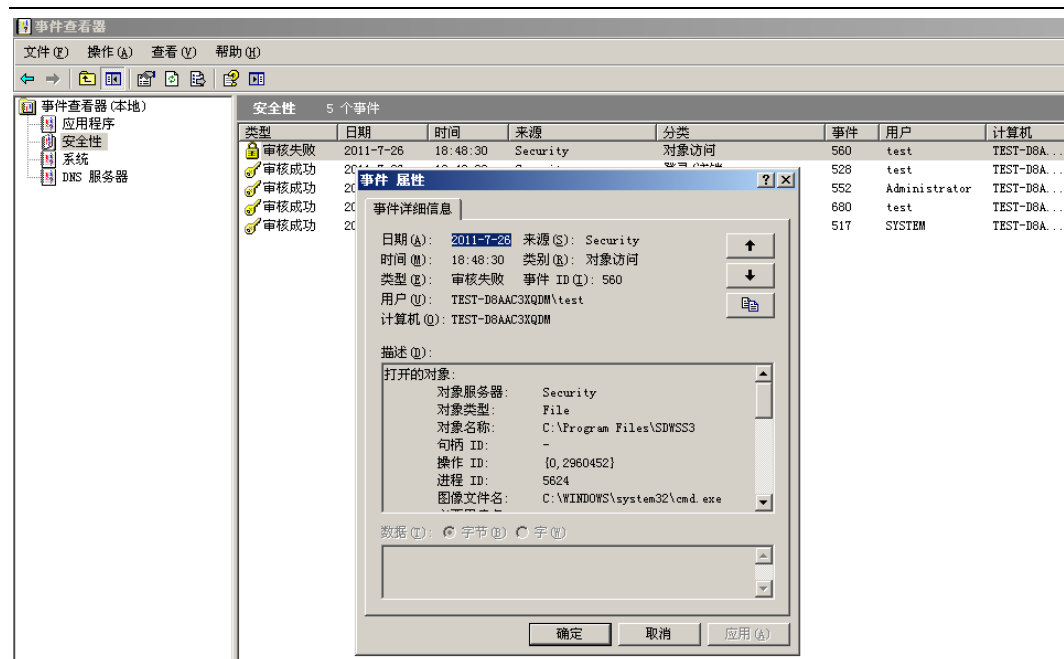
具体示例如下图:



配置完成后,如果有非管理员用户访问产品安装目录,不但会被拒绝,而且会产生一条系统安全审计日志。

二、 查看对象访问审计日志

管理员可以通过打开 " 事件查看器 " 中的 " 安全性 " 查看到对象访问审计日志,如下图所示 :



该日志说明：2011 年 7 月 26 日,18 点 48 分 30 秒,一个叫 test 的非管理员用户试图访问产品安装目录 " C:\Program Files\SDWSS3 ",被系统阻止,且产生了该条日志.

第十二章 卸载产品

一、 卸载前的注意事项

- 1.在卸载开始之前,请**确认 IIS 已经停止运行**(在卸载程序的界面中提供了停止和开启 IIS 的按钮;
- 2.在卸载开始之前,请**确认公共策略和所有私有策略中的 IIS 配置保护已关闭或取消**;

二、 打开卸载程序

点击 " 控制面板 " → " 添加或删除程序 " → " 深空 web 应用防火墙系统 " → " 卸载深空 "

三、 开始卸载

在弹出的对话框中,单击 " 开始卸载(Uninstall) ",卸载过程中程序会提示是否完全卸载,即 " 删除所有配置 " ,如果选择 " 保留配置信息 " ,则配置信息依然保留在计算机中,下次安装时可以直接升级安装即可恢复之前的配置.

卸载完成后单击 " 确定 " 完成卸载.

第十三章 技术支持及联系方式

用户在使用 **深空® web 应用防火墙系统** 过程中遇到任何技术问题,可以通过下列方式与本产品制造商 **福州深空®信息技术有限公司** (FuZhou SkyDeep Information Technology Co.,Ltd)取得联系.

■统一客服热线: 400-0300-630 Tel: 400-0300-630

■传真: 0591-22856511 Fax: 86-591-22856511

■电子邮件: sales##sky-deep.com (把##替换成@)

■E-Mail: sales##sky-deep.com (Replace ## as @)

■统一客服 QQ: 652500285 QQ: 652500285

■公司网址 : www.sky-deep.com Website: www.sky-deep.com

■邮编: 350002 Zip Code:350002

■公司地址:中国 福建省 福州市 鼓楼区 工业路 611 号 福建高新技术创业园 北区 6 楼 东 4

■Addr:East 4,6th floor,North Area,Main Building,Fujian High-Tech Pioneer Park,No.611 GongYe Road,Gulou District,Fuzhou,Fujian,China