深信服虚拟化 Web 应用防火墙云 WAF 用户手册

产品版本	8.0.28
文档版本	01
发布日期	2021-03-12

深信服科技股份有限公司

注意

您购买的产品、服务或特性等应受深信服科技股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，深信服科技股份有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

前言

关于本文档

本文档针对深信服虚拟化Web应用防火墙产品，介绍了云WAF的架构、特性、安装和运维管理。

产品版本

本文档以下列产品版本为基准写作。

产品名称	版本
云WAF	8.0.28

后续版本有配置内容变更时，本文档随之更新发布。

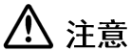
读者对象

本手册建议适用于以下对象：

- 网络设计工程师
- 运维人员

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

图形	文字	使用原则
	危险	若用户忽略危险标志，可能会因误操作发生危害人身安全、环境安全等严重后果。
	警告	该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。
	小心	若用户忽略警告标志，可能会因误操作发生严重事故（如损坏设备）或人身伤害。
	注意	提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。
	说明	对操作内容的描述进行必要的补充和说明。

在本文中会出现图形界面格式，它们所代表的含义如下。

文字描述	代替符号	举例
窗口名、菜单名等	方括号“[ ]”	弹出[新建用户]窗口。
		选择[系统设置/接口配置]。
按钮名、键名	尖括号“< >”	单击<确定>按钮。

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本	发布时间	更新说明
01	2021-03-12	本文档第一次发布。

资料获取

您可以通过深信服官方网站获取产品的最新资讯：

www.sangfor.com.cn

获取安装/配置资料、软件版本及升级包、常用工具地址如下：

bbs.sangfor.com.cn

深信服科技

深信服技术服务

技术支持

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固　话均可拨打）

深信服科技服务商及服务有效期查询：

https://bbs.sangfor.com.cn/plugin.php?id=service:query

意见反馈

如果您在使用过程中发现任何产品资料的问题，可以通过以下方式联系我们。

- bbs.sangfor.com.cn
- 通过联系当地办事处电话反馈
- 售后服务电话 400-630-6430

目录

1. 产品概述

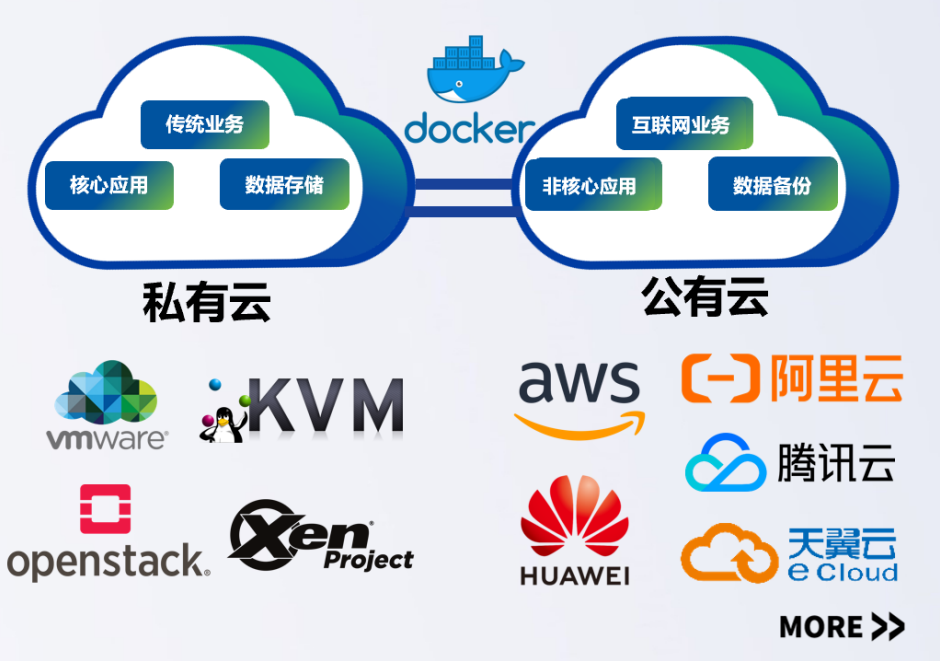
1.1. 产品简介

深信服虚拟化Web应用防火墙（简称云WAF）专注于网站、业务系统、API接口、APP、公众号、小程序等安全防护，解决传统安全产品如网络防火墙、IPS、UTM等安全产品难以应对应用层深度防御的问题，基于攻防情报、机器学习、智能语义技术进行漏斗化高效检测Web攻击，满足OWASP TOP 10 防护需求和符合监管要求。提供贴合业务的多重手段，帮助用户建设适用业务需求的安全防线，并通过多种智能分析技术和联动组件持续对抗各类新型攻击。实现用户Web业务应用安全与可靠交付。

1.2. 产品关键特性

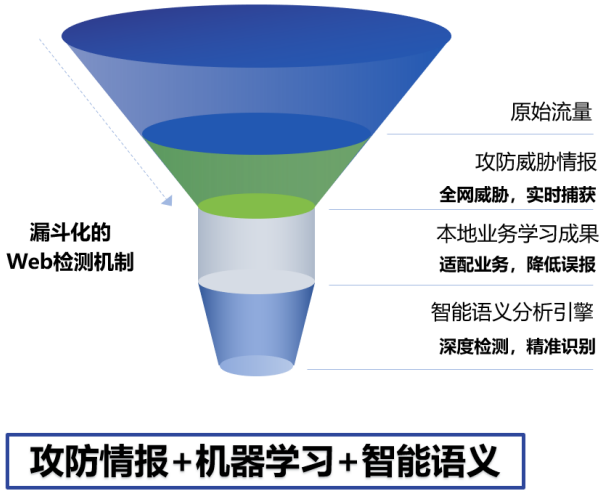
一、 支持多种环境部署

深信服虚拟化Web应用防火墙为云而生，可以在虚拟机、容器和云平台上部署，广泛兼容各类私有云和公有云，如阿里云、华为云、腾讯云和天翼云等。以软件的形式部署在centos7/8的docker环境中。



二、 规则+三重高效漏斗检测模型

深信服虚拟化Web应用防火墙基于自研的正则引擎和安全团队持续迭代的安全规则，搭载攻防情报、机器学习、智能语义等智能引擎建立规则+三重高效漏斗化检测机制，实现Web攻击精准检测，有效降低误判漏判。



深信服WAF漏斗检测模型

三、 支持反向代理

当客户的网络环境比较复杂时，不需要改变网络结构的需要有也能提供多种部署方案，方便WAF适应更多场景和灵活部署。通过反向代理的部署方式，隐藏真实的服务器地址从而防止真实的服务器遭受攻击。也能根据业务流量大小，对流量进行负载分担到各个服务器上去解决负载不均衡问题和保障业务的稳定性。

四、 Bot防护

Bot防护引入动态JS指纹行为，识别访问的客户端是否为扫描器或正常客户端，并对其请求进行认证，以达到人机区分来阻断恶意攻击者的扫描行为。从而解决客户遇到的扫描器等自动化攻击问题。Bot防护功能有效识别和管理爬虫、脚本程序，阻挡自动化攻击如信息探测、漏洞扫描、CC攻击等。拦截黑灰产业如薅羊毛、批量注册等危害业务数据安全的攻击；缓解业务应用网络资源压力。

五、 支持SSL加解密

随着越来越多的数据泄露事件披露，网络安全和隐私问题成为信息安全的雷区，HTTP在网络传输过程中是明文，数据包很容易被劫持，导致信息泄露。HTTPS加密则解决了传输过程中信息被泄露的可能，但Web攻击仍然存在，所以需要部署支持HTTPS解密功能的Web应用防火墙进行解密。WAF反向代理支持HTTPS解密，从而防护网站免受攻击。业务系统都是使用HTTPS协议，客户端访问服务器全程使用HTTPS协议传输，WAF支持HTTPS解密，对经过WAF的HTTPS流量进行解密和安全检测。

2. 安装部署

本节主要写作安装前的准备工作，包括准备工具、环境、软硬件材料等。

2.1. 安装前准备

2.1.1. 环境要求

操作系统：Centos 7/8

说明：

支持 OVA、qcow2 的形式导入到虚拟化或者云平台。

2.1.2. 配置要求

深信服虚拟化Web应用防火墙需要根据实际应用层吞吐量来配置设备的性能，具体配置需求参数如下：

表1 云WAF虚拟机推荐配置

CPU	内存	硬盘	应用层吞吐
2 核	4G	100G	100M
2 核	4G	100G	200M
4 核	8G	100G	400M
4 核	8G	100G	800M
8 核	16G	100G	1600M

2.1.3. Web 控制台登录介绍

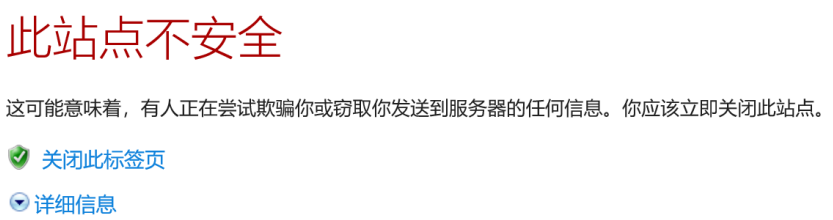
虚拟化Web应用防火墙支持安全的HTTPS登录，是使用HTTPS协议的非标准端口登录，为了防止配置过程中被截获而产生安全隐患。

如果需要登录Web控制台，需要保证电脑与安装的云WAF直接网络能够正常访问，输入https://IP:4431，即可正常登录设备。

操作步骤

步骤1. 首先为本机器配置一个IP，然后在IE浏览器中输入网址：https://IP（云WAF地

址）:4431。出现一个如下图的安全提示，点击<详细信息>再点击<转到此网页>会跳转到控制台登录页面。



步骤2. 在登录框输入用户名和密码，默认情况下用户名和密码均为：admin。勾选我已阅读并同意，点击<登录>按钮即可登录云WAF设备进行配置。

2. 2. 部署模式

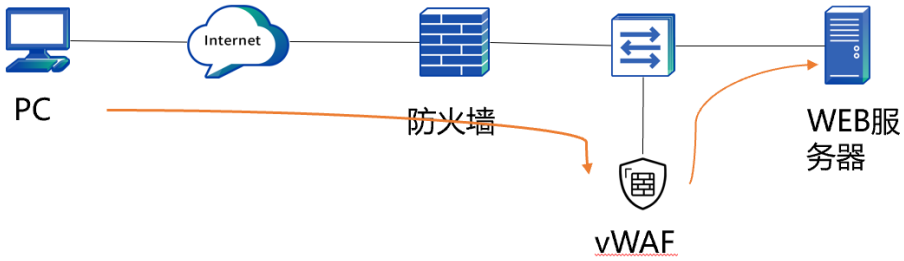
部署模式是用于设置设备的工作模式，可把云WAF设定为单机模式、集群模式。选择一个合适的部署模式，顺利将云WAF架到网络中并且使其能正常使用的基础。

表2 部署模式说明表

部署模式	场景说明
单机模式	云 WAF 通过反向代理功能对所有的流量进行代理，并保护业务站点，从而更加贴合业务。
集群模式	单台云 WAF 不能满足业务的需求，需要进行扩容来提升设备的性能。该方案需要配合负载均衡设备引流的形式来对流量分发到各个云 WAF 上，从而大流量的业务进行安全防护。

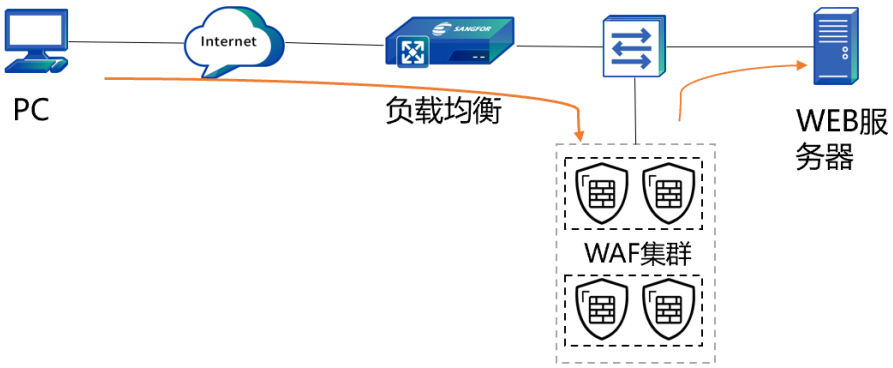
2.2.1. 单机模式

云WAF部署在客户虚拟环境或者云平台中，防火墙通过目的地址映射，将公网的Web服务器IP转换成云WAF的IP和端口。流量到达云WAF后，匹配对应的虚拟服务，将流量负载到各个节点业务服务器上。在整个过程中，云WAF起到反向代理作用，并对流量进行安全防护。



2.2.2. 集群模式

企业环境中，部署多台云WAF为了解决业务的可靠性和弹性伸缩需求，通过负载均衡设备把业务流量负载到各个云WAF中，流量到达云WAF后，匹配对应的虚拟服务，将流量负载到各个节点业务服务器上。为了能够承载更大的业务流量，可以增加多台云WAF，只需要在负载均衡设备中将云WAF添加到对应的组中即可。

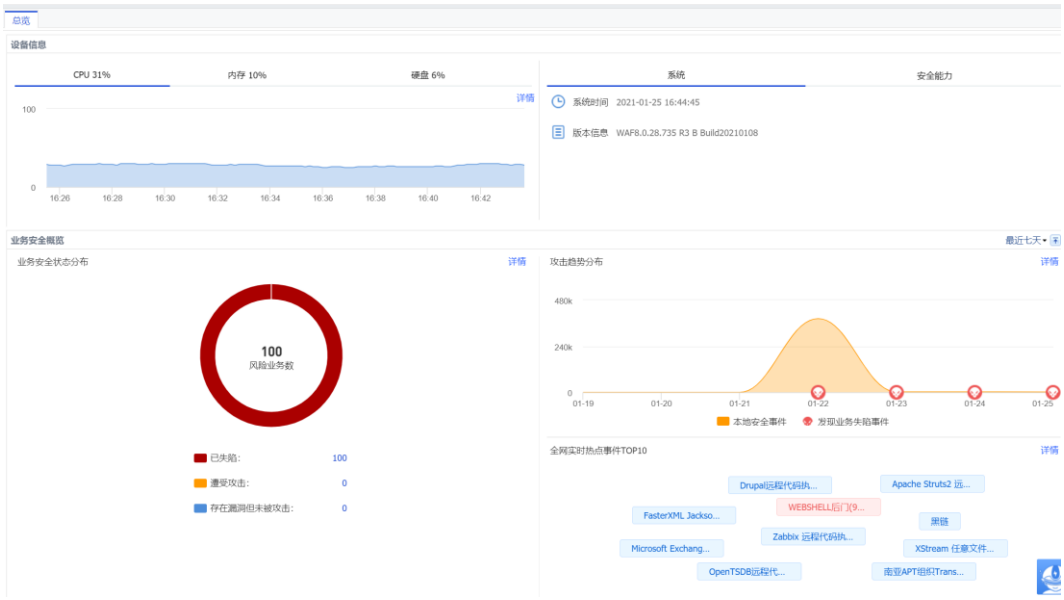


3. 运行状态

运行状态的功能主要是查看当前设备的运行状况、业务安全防护和云端黑客IP防护等，能够及时反应全网当前攻击信息。

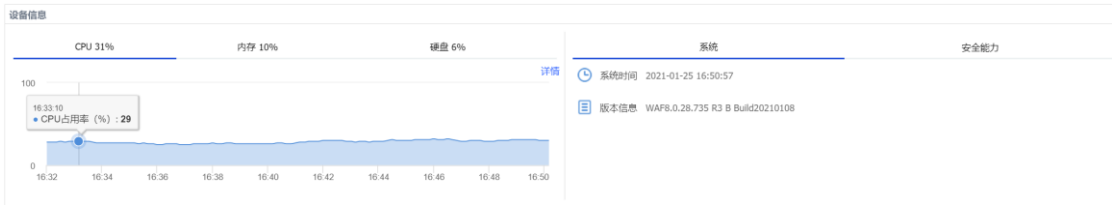
3.1. 总览

主要展示设备的运行状态、系统、安全能力和业务防护等信息，如下图所示。



设备信息

显示设备运行状态下CPU、内存、硬盘的使用情况，便于查看设备运行是否在合理范围之内。



点击<详情>，可以查看CPU、内存和磁盘实时/最近24小时/7天的具体使用情况。

系统：显示当前设备时间和版本信息。

安全能力：显示当前设备开启的那些安全能力功能，当鼠标停留在对应的安全功能时，可以查看具体的序列号过期的时间。

业务安全概览

业务安全概览提供迅速掌握业务整体的安全状况（业务安全状态分布、攻击事件趋势、全网实时热点事件TOP10）。如下图所示。

点击 ，可以将此栏置顶显示。

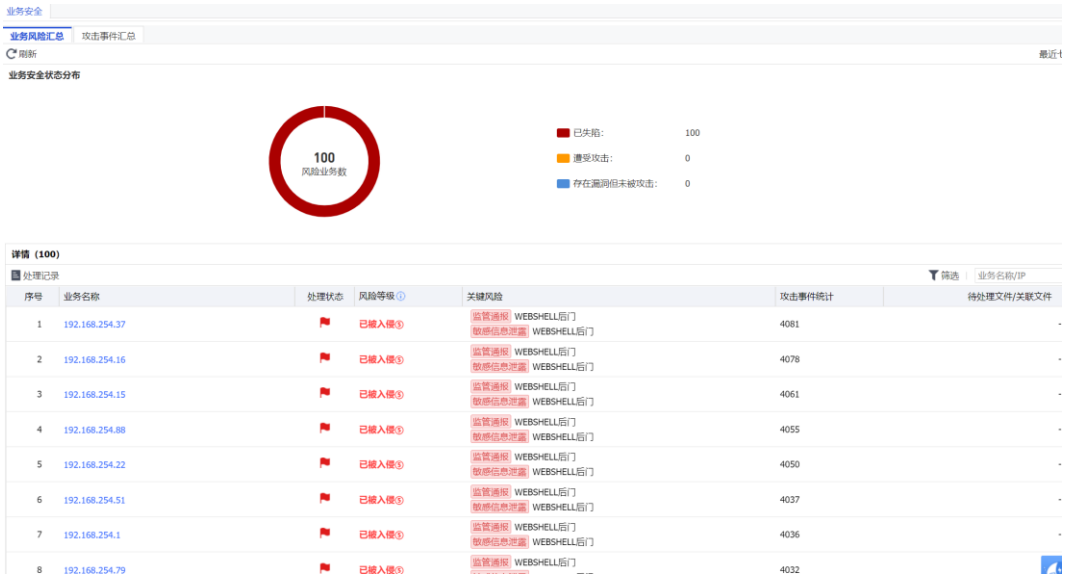
点击下拉框，可以选择最近七天、最近两天和今天的时间范围的信息。

3.2. 业务安全

业务安全是从业务角度进行安全展示，掌握网络中业务相关的整体安全状况，包括业务风险汇总和攻击事件汇总攻击二个功能模块。

3.2.1. 业务风险汇总

业务风险汇总是从业务角度进行安全展示。可以查看到业务是否存在被攻击或者看到潜在的风险。如下图所示。



关于风险等级说明，可以参考如下表。

表3 风险等级说明表

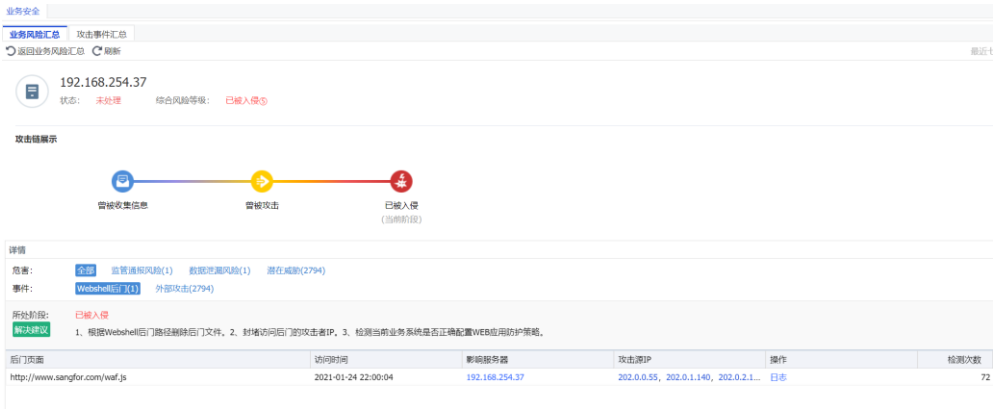
风险等级	说明

已被入侵	已有数据证明服务器已被黑，如被挂 Webshell、黑链等
曾被攻击	无数据证明服务器被黑，但存在被攻击的证据：包括 SQL 注入、暴力破解、Webshell 上传等攻击类型的日志
曾被收集信息	无数据证明服务器被黑，但存在被搜集信息的证据
存在漏洞	无数据证明服务器被黑，无被攻击记录，但服务器本身存在漏洞

关键风险类型包含：监督风险、敏感信息泄露、公众形象受损，高中低危漏洞。漏洞统计是基于实时漏洞分析的结果进行统计。

点击<筛选>，可根据综合风险等级进行筛选。如下图所示。

点击业务名称即可进入安全详情，跳转后如下。

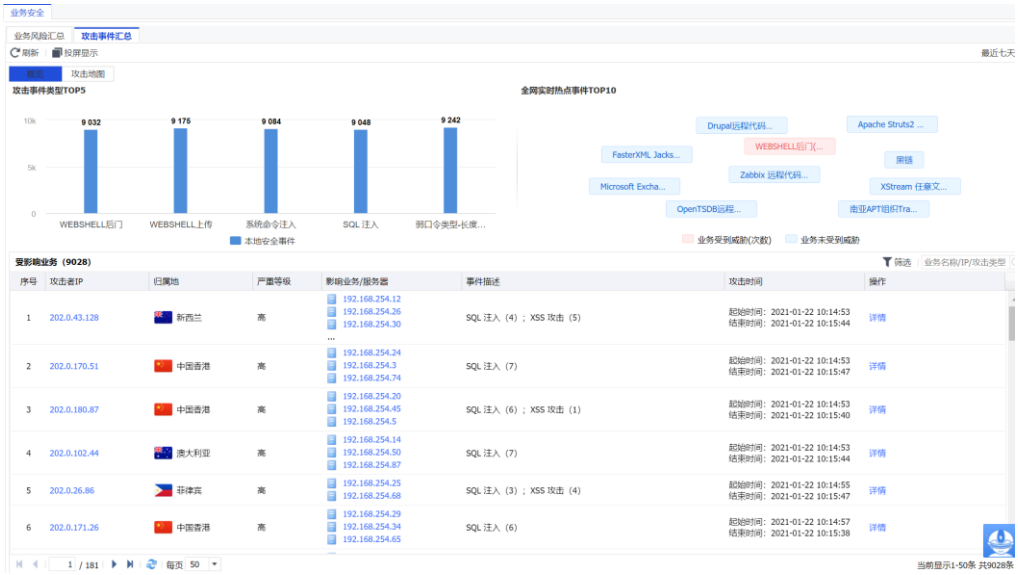


如图，上半部分该业务的安全总览，详情项包括：该业务当前所遭受的危害，造成该危害的具体事件类型（Webshell文件访问、Webshell后门、僵尸网络活动、内部漏洞、外部攻击等）。

所处阶段：已被入侵；影响的服务器，解决建议，以及举证。

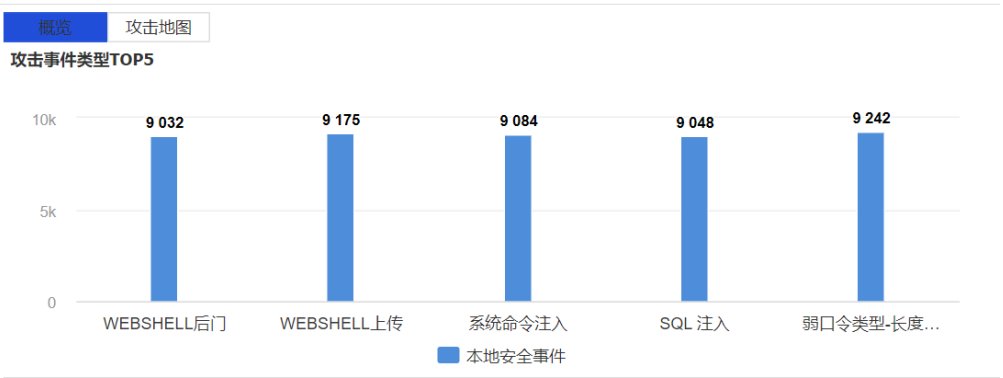
3.2.2. 攻击事件汇总

攻击事件汇总该页面是从攻击者角度进行安全展示。可看到攻击事件类型TOP5和攻击者地图。如下图所示。

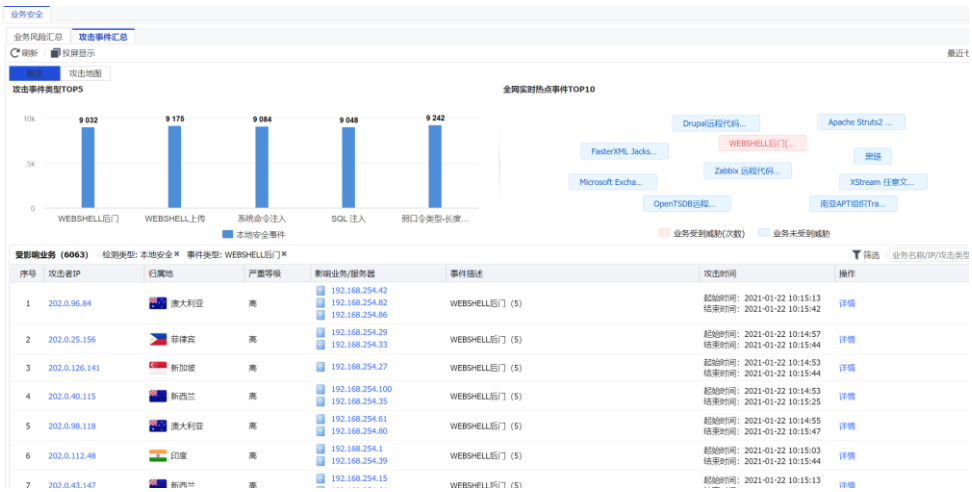


攻击事件类型

攻击事件类型展示的是最近攻击事件TOP5的类型。如下图所示。



点击攻击事件具体类型，可在表格中过滤出该攻击事件类型相关的日志。



攻击者地图

攻击者地图用于显示云WAF设备今天/最近两台/最近7天检测到的攻击者的IP来源。

点击<投屏显示>，跳转到攻击者地图展示页面。如下图所示。

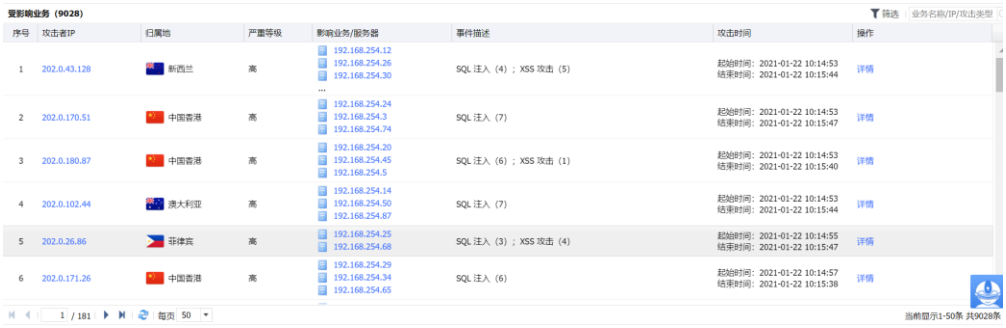
全网实时热点事件

全网实时热点事件TOP10是根据当前业务方面的热点事件进行整理，结合客户当前的攻击日志来分析，看客户业务是否有遭受热点事件的攻击。红色表示业务已发生，灰色表示业务未发生。如下图所示。

点击具体热点事件，可在表格中过滤出具体的日志。如下图所示。

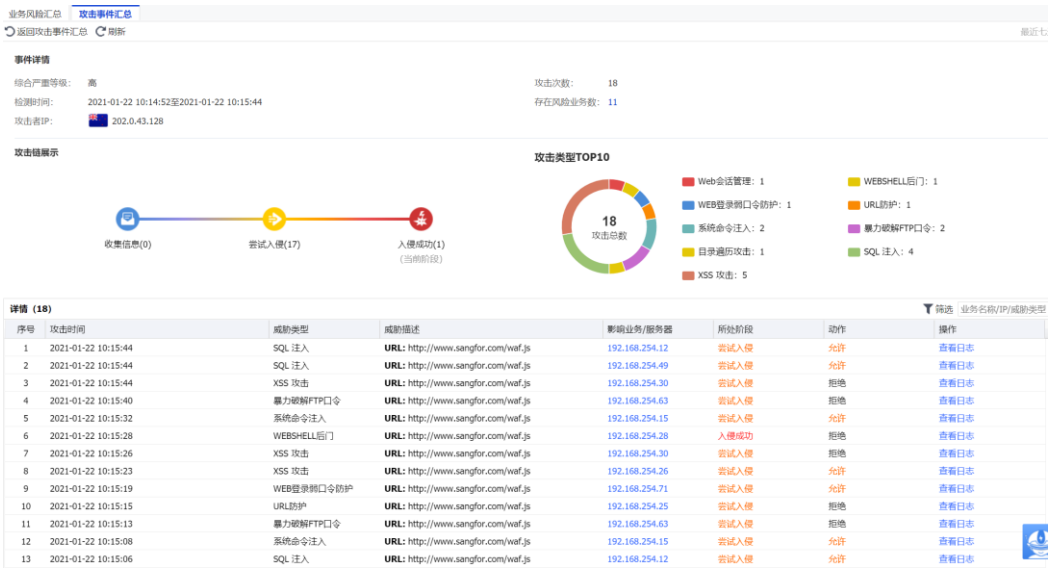
受影响业务

受影响业务主要用于显示最近发生的攻击事件，如下图所示。



如图，显示的内容包括：攻击者IP、归属地、严重等级、影响业务/服务器、事件描述、攻击时间、状态以及操作。

点击具体的攻击者IP，可查看该攻击IP对客户业务的威胁情况（事件详情、攻击链展示、攻击类型TOP10）。如下图所示。



点击<筛选>，可根据所处阶段、影响业务和动作进行筛选。如下图所示。

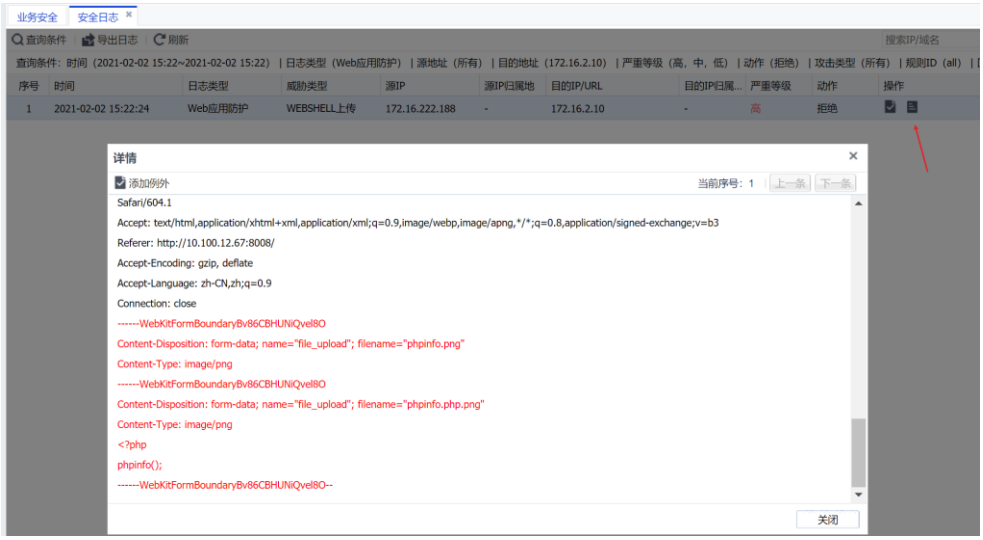
处置案例

某用户发现内网较多核心服务器遭受严重的攻击，需要进行分析是否为误判。

步骤1. 查看遭受攻击的服务器，如下图所示。

步骤2. 点击详情查看具体的攻击行为，并对日志进行分析，如下图所示。

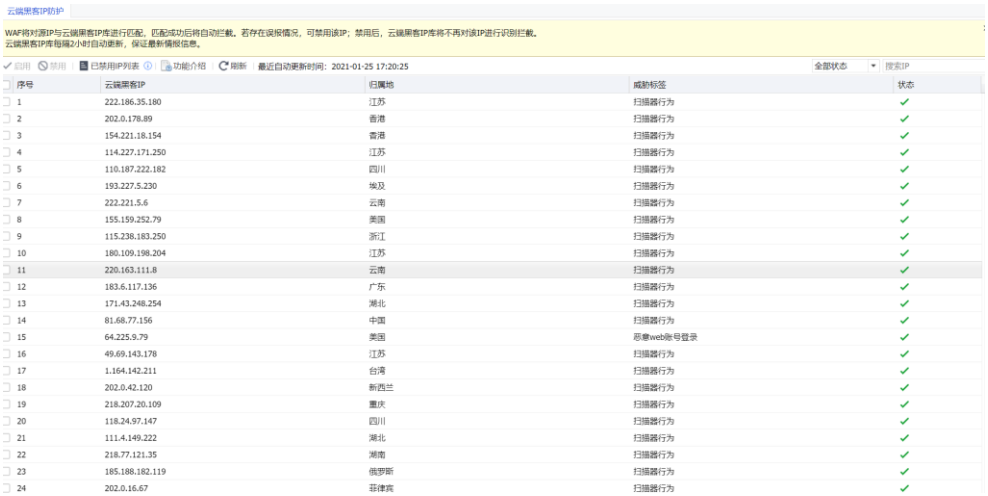
步骤3. 点击查看日志，对具体的日志进行分析，如下图所示。



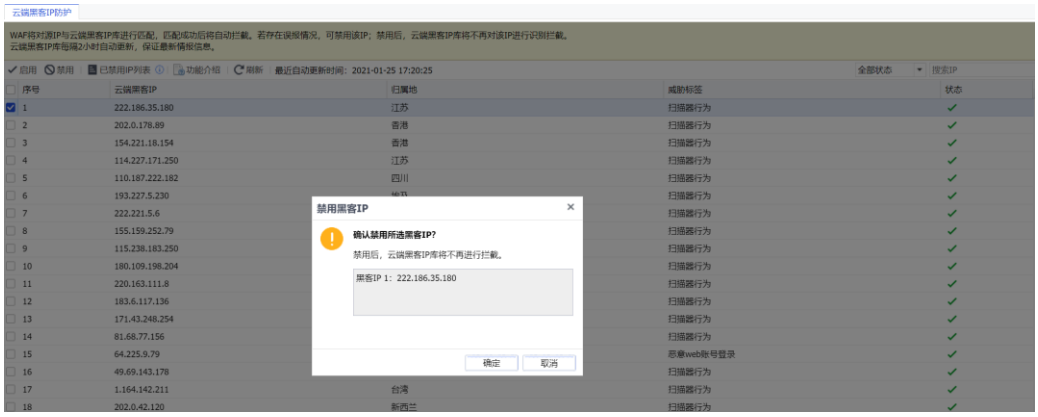
步骤4. 经日志分析，该行为是真实攻击WebSHELL上传，确定后可在互联网出口设备对该源IP地址进行封锁。

3.3. 云端黑客 IP 防护

云端黑客IP防护是云WAF连接到云端，通过主动拉取云端的黑客IP同步到本地，对防护列表中黑客IP进行防护。当黑客IP流量经过vWA后，匹配成功的源IP将自动拦截。若存在误报情况，可禁用该IP；禁用后，云端黑客IP库将不再对该IP进行识别拦截。云端黑客IP库每隔2小时自动更新，保证最新情报信息。



如果存在误报，勾选对应得IP，点击<禁用>，弹出确认按钮，点击<确定>，即可禁用该黑客IP。如下图所示。



说明：

如需要开启云端黑客 IP 防护，需要云 WAF 能够连接到互联网。

4. 监控

监控功能可以查看设备产生的所有日志，是云WAF的日志中心。

4.1. 日志

在安全设备运行中，会产生大量的系统和安全日志。日志功能主要记录设备产生的安全和系统日志。方便用户对日志进行查看、分析。日志存储方式有防火墙（本地）、安全感知系统和syslog三种方式，防火墙默认存储日志在本地上，主要受设备磁盘大小制约。为了满足合规要求推荐防火墙加态势感知系统的形式存储日志，一是满足合规备份存储的需求，二是态势感知系统能够存储海量日志和帮助溯源分析等。

4.1.1. 安全日志

安全日志主要记录业务攻击的行为，包括Web应用防护和Web漏洞。触发安全日志会记录源目IP、源目端口、日志类型、时间、动作等信息，可以对日志进行导出，然后进行分析或者在搜索框中输入IP/域名进行搜索对应得日志信息。如下图所示。

安全日志检索案例

某企业网络管理员发现Web服务器正遭受攻击，需要查看Web防护日志、确定攻击的IP和攻击使用的手段等信息。

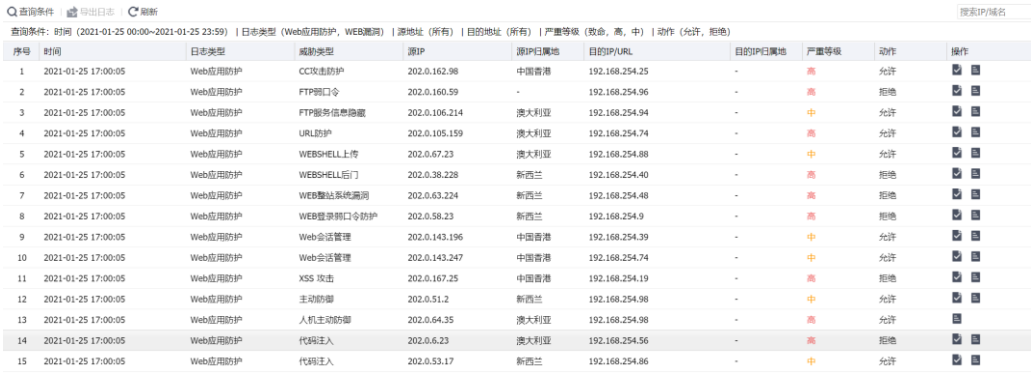
步骤1. 点击<查询条件>，根据需求选择搜索的条件，如下图所示。

表4 日志查询条件说明

查询条件	说明
起始/结束时间	选择查询开始至结束的时间
源地址	攻击者的来源 IP
目的地址	攻击者攻击的 IP
日志类型	选择 Web 应用防护和 Web 漏洞
严重等级	根据不同的安全级别进行筛选
动作	根据日志的动作进行筛选

步骤2. 根据需求选择对应的时间日期，勾选Web应用防护和Web漏洞，查看Web应用防护和Web漏洞日志，如下图所示。

步骤3. 查看Web应用防护日志，如下图所示。



步骤4. 点击<查看详情>，查看攻击行为是否为误报，如下图所示。

可以根据查看日志的详细信息判断是否为误报，如果为误报则添加到例外。例外添加在日志最右端操作界面上，点击<添加例外>，弹出对话框。

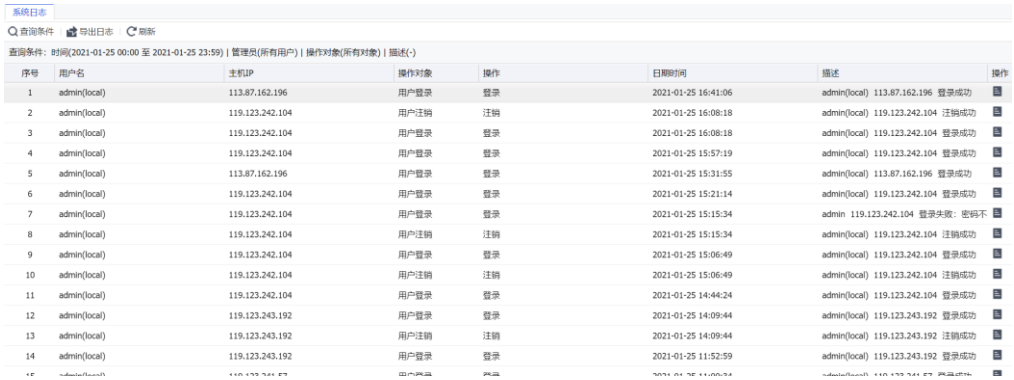
URL：需要匹配的URL。

排除例外：对匹配上的源目IP、目的端口、规则ID进行添加例外。

仅排除参数值符合以下特征需求：Web应用防护的网站攻击检测将跳过这些参数的检查。主要用于正常业务下某些请求参数因携带特征串而被检测为攻击的情况，可以只针对这些参数排除。

4.1.2. 系统日志

系统操作用于查询用户登录控制面板的登录注销日志以及所做过的所有操作日志，例如可以查询出admin这个账号在某天登录控制台做过哪些操作。



系统日志检索案例

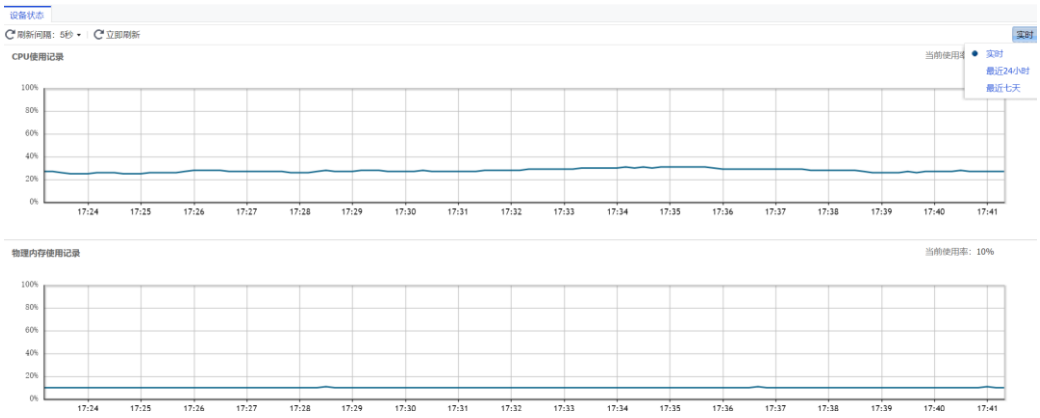
某企业网络中，需要检索近期哪些管理员账号配置Web应用防护的情况。

步骤1. 点击<查询条件>，对Web应用防护的配置情况进行检索，如下图所示。

步骤2. 查看检索结果，列出了进行Web应用防护配置的管理员账号、操作时间、主机等信息。

4.2. 状态

状态功能记录实时/最近24小时/最近7天的CPU和物理内存的使用情况，方便观察平台在某段时间内的CPU和物理内存的使用量，如下图所示。

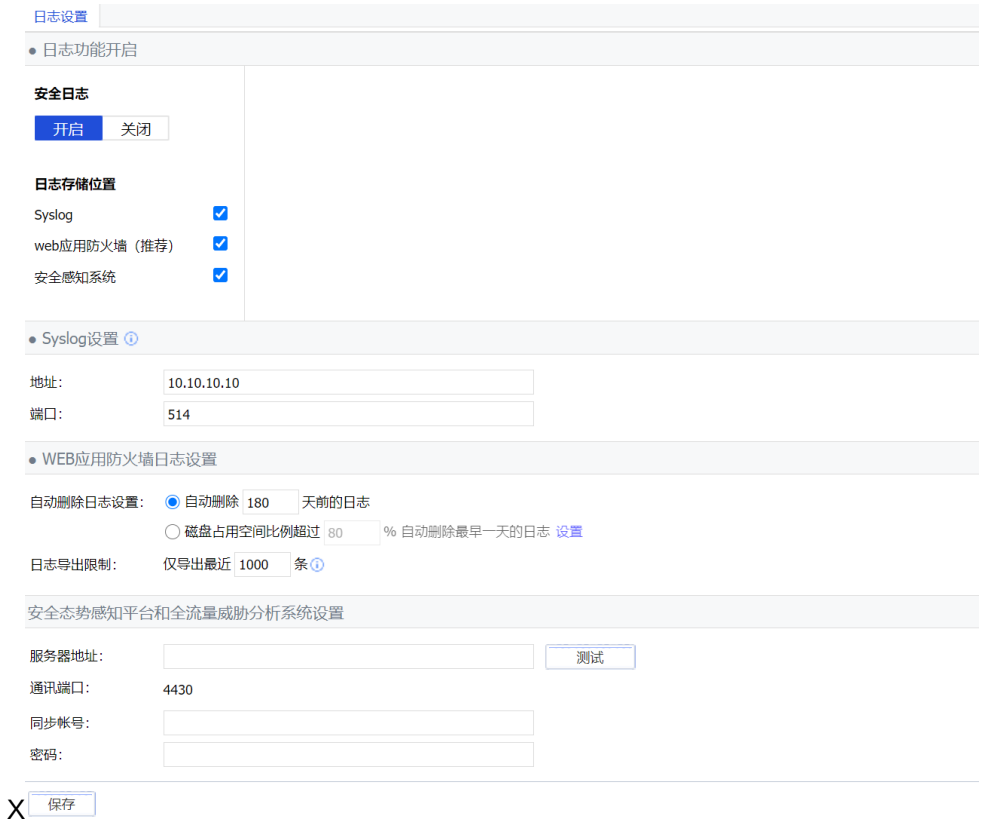


4.3. 设置

设置功能主要对日志存储功能进行设置，并对日志是否告警配置等，是一个日志功能开关的集合。

4.3.1. 日志设置

日志设置功能主要控制设备日志的启停，并控制着设备产生的日志存储到第三方设备上。从而满足日志存储的合规要求，界面如下。



4.3.1.1. 日志功能开启

日志功能开启后，设备才能够记录日志到指定的位置，如syslog、Web应用防火墙、安全感知系统。可记录安全日志，个别默认是关闭的，如果需要开启，需要在页面中勾选相应的选项开启。默认推荐只开启安全日志存储到本地。

4.3.1.2. SYSLOG 设置

在安全设备运行中，会产生大量的系统、安全和运行等日志。而安全设备本身的存储空间无法满足日志的存储，易造成日志覆盖或者丢失，导致无法进行攻击溯源分析和满足监管要求。因此，安全设备与Syslog服务器对接成功后，安全设备发送日志给Syslog服务器，从而减轻了安全设备的日志存储压力和满足监管的合规要求。

Syslog用于将设备日志发送到Syslog服务器进行存储，需要设置Syslog服务器的IP和端口信息。

SYSLOG配置案例

某企业云平台中，部署了一台云WAF。为满足监管要求，需要把安全日志发送到日志服务器上进行存储，且该服务器只能接收UDP514的数据包。

步骤1. 开启安全日志通过syslog的形式发送，如下图所示。

步骤2. 配置syslog服务器，并以UDP514的形式发送日志给日志服务器，如下图所示。

步骤3. 查看云WAF产生安全日志,查看日志详情，并是否把日志发送给syslog服务器，如下图所示。

步骤4. 日志能够发送到syslog服务器。

说明：

1.SYSLOG 仅支持 UDP 方式连接，UTF-8 的编码方式。
2.系统日志不能发送到 syslog 服务器。

4.3.1.3. Web 应用防火墙日志设置

用于设置设备存储日志的自动删除选项，页面如下。

自动删除日志设置：用于设置是否需要系统自动删除已记录的访问控制日志，选择自动删除此天数前的日志用于设置按天数来保存日志，选择磁盘占用空间超过此比例则自动删除最早一天的日志用于设置按磁盘占用率来保存日志。

日志导出限制：允许导出的日志条数，导出的日志过多会消耗大量内存和CPU等资源。

⚠ 注意：

已删除的日志无法找回，建议增加外置的 syslog、态势感知系统等进行日志备份。

4.3.1.4. 安全态势感知平台和全流量威胁分析系统设置

主要用于设置设备与安全感知系统和全流量威胁分析系统联动，联动后云WAF的日志会同步到态势感知平台上，并将日志进行溯源分析等。态势感知平台也可以下发指令给云WAF，云WAF收到指令后执行对应的动作。如下图所示。

服务器地址：是安全感知系统和全流量威胁分析系统的地址。

通讯端口：默认4430端口。

同步账号：接入安全感知系统和全流量威胁分析系统的账号信息。

密码：接入安全感知系统和全流量威胁分析系统的密码信息。

4.3.2. 告警设置

当设备发生异常行为或者存在攻击行为进行时，以邮件的方式进行告警，从而能够让客户快速感知到目前的网络情况。

4.3.2.1. 告警事件

选择需要开启告警的事件，勾选即开启告警，如下图所示。

4.3.2.2. 告警通知

告警通知目前仅支持邮件的形式进行告警。当设备检测出设备触发到告警事件，根据设置邮件告警的方式告知管理员。如下图所示。

邮件通知设置

用于设置将告警信息以邮件的形式发送到管理员邮箱。例如当内网有病毒，或磁盘空

间存储到一定比例的时候，设备会自动发送告警邮件到管理员邮箱，达到提醒告警的目的。点击<设置邮件服务器>，可以进行邮件服务器的设置。

4.3.2.3. 邮件告警设置案例

某企业环境中，部署了一台云WAF，先需要对高危的安全事件进行邮件告警，从而使管理员能够快速的响应。

步骤1. 云WAF能够访问互联网，且配置邮件服务器，如下图所示。

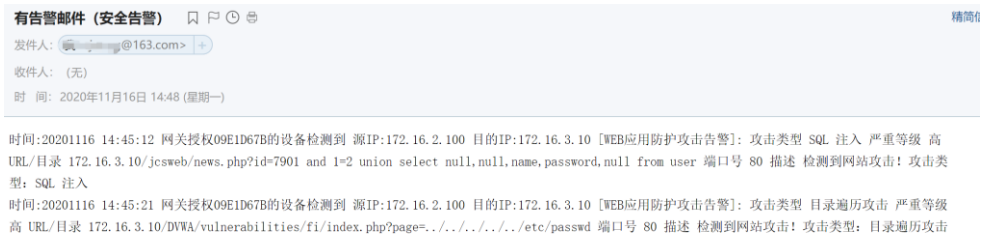
注意：

若您配置的发件邮人邮箱已启用第三方客户端授权码，请在此输入授权码。

步骤2. 在[监控/设置/告警事件]开启告警功能，对需要出发的事件进行告警提示。

步骤3. 设置邮件告警，并填写对应的告警邮箱，如下图所示。

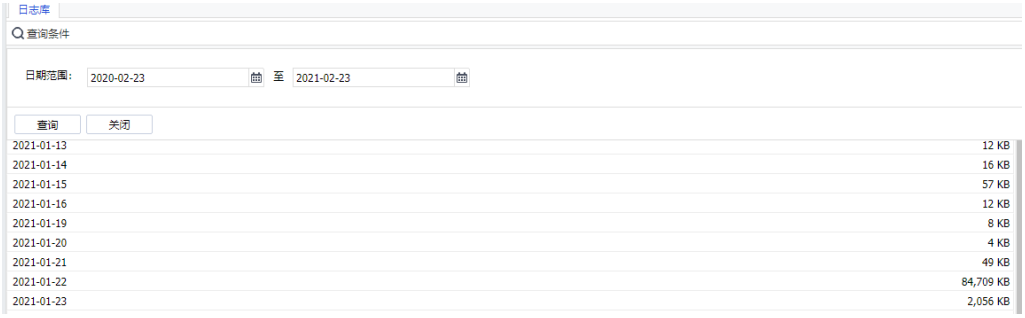
步骤4. 查看遭受攻击后，收到的告警内容，如下图所示。



4.3.3. 日志库

日志库可以根据日期范围来查询指定时间日志。

设置好查询日志范围，点击<查询>，设备会查询出指定日期范围内的日志，页面如下。



5. 对象

对象定义中的各种对象是云WAF做安全防护的基础设置， Web应用防护策略是基于对象来引用的，所以不同的业务可以创建不同的对象，便于进行精细化的策略调整。

表5 对象定义功能说明

功能类别	功能说明
安全策略模板	用户可以设置安全模板的内容，安全模板提供给安全策略引用。
安全防护规则	用户可以查找对应的安全规则，也可以自定义规则。这些规则汇总起来提供给安全模板进行引用。

5.1. 安全策略模板

主要集合安全规则整合到一个模板中，让安全策略进行调用，可根据不同的业务的需求进行调整。

5.1.1. Web 应用防护

Web应用防护是专门针对内网的Web服务器设计的防攻击策略，可以防止系统命令注入、SQL注入、XSS攻击等各种针对Web应用的攻击行为，以及针对Web服务器进行防泄密设置。如下图所示。

默认模板：默认开启常规的Web防护功能，但不开启“漏洞防扫描功能”。

默认模板II：默认开启常规的Web防护功能，同时开启“漏洞防扫描功能”。

点击<新增>，可以创建Web应用防护模板，如下图所示。

模板名称：定义该模板的名称。

描述：定义对该模板的描述。

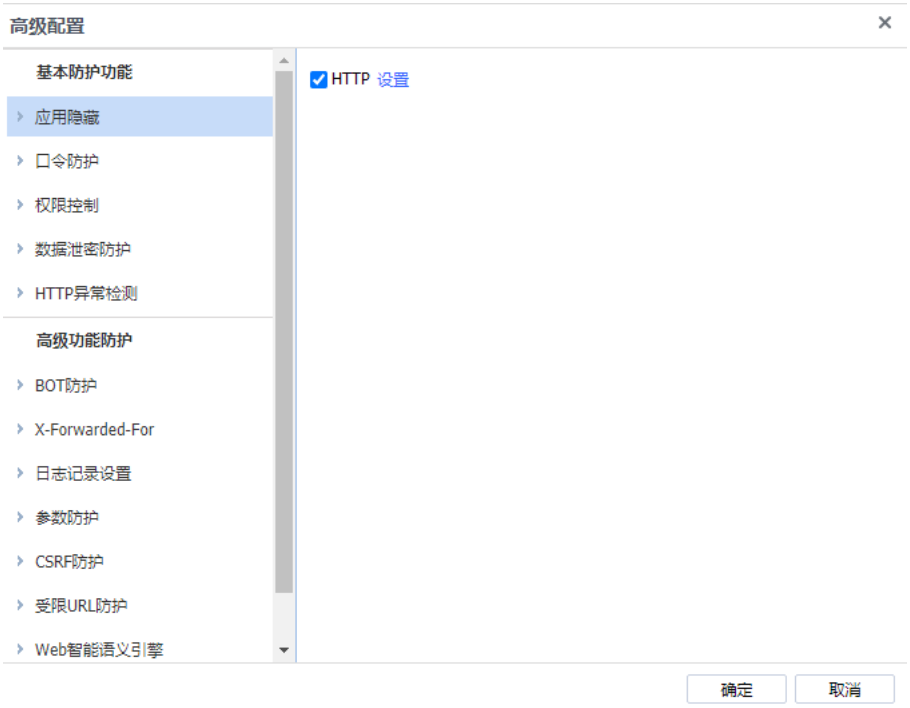
防护类型：设置针对服务器的哪些攻击行为进行防护。点击<防护类型：SQL注入、XSS攻击、网页木马等>弹出选择Web应用防护类型编辑框，勾选相应的防护类型，则设备会对这一种服务类型的相关攻击行为进行防护。

表6 Web应用防护类型说明

防护类型	说明
SQL 注入	攻击者通过设计上的安全漏洞，把 SQL 代码粘贴在网页形式的输入框内，获取网络资源或改变数据。

XSS 攻击	跨站脚本攻击，XSS 是一种经常出现在 Web 应用中的计算机安全漏洞。它允许代码植入到提供给其他用户使用的页面中。例如 HTML 代码和客户端脚本，攻击者利用 XSS 漏洞绕过访问控制，获取数据，例如盗取账号等。
网页木马	网页木马是一个经过黑客精心设计的 HTML 网页。当用户访问该页面时，嵌入该网页中的脚本利用浏览器漏洞，让浏览器自动下载黑客放置在网络上的木马并运行这个木马。
网站扫描	网站扫描是对 Web 网站扫描，对 Web 网站的结构、漏洞进行扫描。
WebShell	WebShell 是 Web 入侵的一种脚本工具，通常情况下是一个 ASP、PHP 或者 JSP 程序页面，同时也称为网站后门木马，在入侵一个网站后，常常将这些木马放置在服务器 Web 目录中，与正常网页混在一起。通过 WebShell 来长期操纵和控制受害者网站。
跨站请求伪造	通过伪装来自受信任用户的请求来利用受信任的网站。
系统命令注入	攻击者利用服务器操作系统的漏洞，把 OS 命令利用 Web 访问的形式传至服务器，获取其网络资源或者改变数据。
文件包含攻击	文件包含漏洞攻击是针对 PHP 网站特有的一种恶意攻击。当 PHP 中变量过滤不严，没有判断参数是本地的还是远程主机上时，就可以指定远程主机上的文件作为参数来提交给变量指向，当提交的文件存在恶意代码或木马时，文件中的代码和木马会以 Web 权限被成功执行。
目录遍历攻击	目录遍历漏洞就是通过浏览器向 Web 服务器任意目录附加“../”，或者是在有特殊意义的目录附加“../”，或者是附加“../”的一些变形，编码访问 Web 服务器的根目录之外的目录。
信息泄露攻击	信息泄露漏洞是由于 Web 服务器配置或者本身存在安全漏洞，导致一些系统文件或者配置文件直接暴露在互联网中，泄露 Web 服务器的一些敏感信息，如用户名、密码、源代码、服务器信息、配置信息等。
Web 整站系统漏洞	针对知名 Web 整站系统中特定漏洞进行安全可靠高质量防护。
WebShell 后门通信	在已知Web系统漏洞情况下，攻击者利用Web系统漏洞将WebShell页面成功植入到Web系统中，攻击者通过WebShell页面访问数据库，执行系统命令并长期的操控Web系统。
自定义 W 云 WAF 规则	用户可自定义防护规则，对服务器进行防护，自定义规则在自定义规则中进行设置。
Web 漏洞攻击	对Web服务器的漏洞进行安全防护和检测。

防护功能：主要功能有应用隐藏、口令防护、权限控制、数据防泄密、HTTP异常检测、BOT防护，开启高级的防护功能请点击<高级配置>中进行设置。



5.1.1.1. 应用隐藏

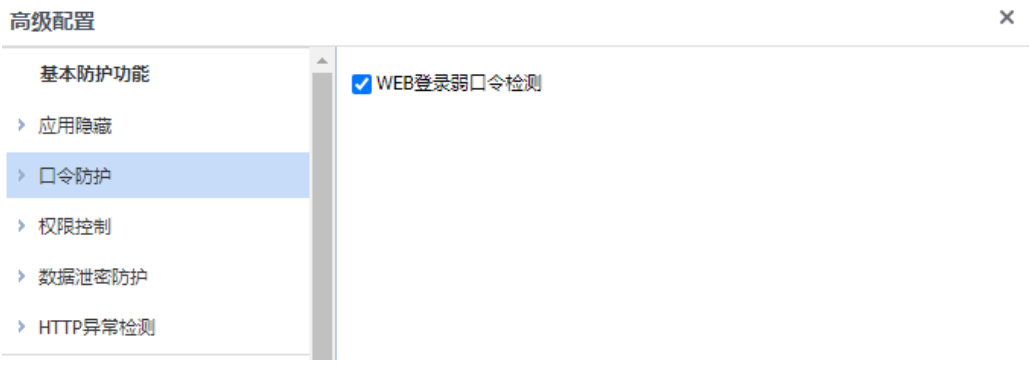
HTTP：当客户端访问Web网站的时候，服务器会通过HTTP报文头部返回客户端很多字段信息，例如Server、Via等，Via可能会泄露代理服务器的版本信息，攻击者可以利用服务器版本漏洞进行攻击。因此可以通过隐藏这些字段来防止攻击。勾选HTTP，点击<设置>，弹出的页面如下。

启用过滤HTTP响应报文头，需要自定义HTTP报文头的内容，可以利用HTTPWATCH

等抓包工具获取该服务器返回客户端的一些字段，并且填写到此处。勾选替换HTTP出错页面，则针对一些错误页面，例如服务器返回500错误的页面（该页面通常包含服务器信息），防火墙会用一个不包含服务器信息的错误页面来替换原始的错误页面。

5.1.1.2. 口令防护

Web口令防护设置：该防护针对http协议有效。主要是针对一些过于简单的用户名密码进行过滤，点击<口令防护>，弹出如下页面。



勾选Web登录弱口令，点击<确定>保存设置即可。当防火墙检测到这种弱口令会产生日志记录提醒管理员。

5.1.1.3. 权限控制

文件上传过滤：主要是用于过滤客户端上传到服务器的文件类型，勾选文件上传过滤，点击<设置>，弹出的页面如下。

点击下拉框可以下拉选择设备内置的一些文件类型，点击+号，则添加到列表。如果要自定义的类型，可以直接在框里输入自定义的文件类型，点击+，则添加到列表。

URL防护：该设置的主要功能是权限开关。例如禁止访问某个URL，则上述的防攻击等都无效，因为客户端都无法访问，更不会存在攻击。如果此处允许某个URL，则上述设置的防攻击等针对该URL都会无效，相当于一个白名单。勾选URL防护，点击<设置>，页面如下。

点击<添加>，增加URL过滤，如下图所示。

此处的填写方式与防爆破类似，需要填写URL的后缀。例如某URL为http://www.***.com/admin ，则此处填写/admin，并根据需求对该URL进行拒绝或者允许访问。如果勾选记录日志，则对访问该域名URL的地址将会记录到安全日志中，方便用户查看哪些源IP对该URL进行访问。

5.1.1.4. 数据库泄密防护

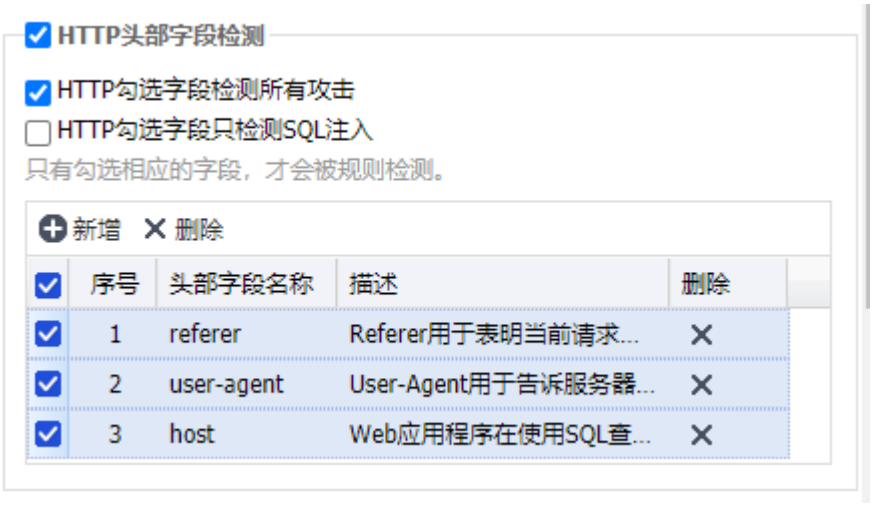
文件下载过滤：由于某些敏感信息是以word或者是excel等文档形式保存的，通过从服务器上下载文档把这些敏感信息泄露出去，对于这种泄露方式，可以通过过滤文件下载来进行防护。

勾选文件下载过滤，点击<设置>按钮，弹出设置过滤文件类型编辑框，选择需要过滤哪些文件后缀，页面如下图所示。

设备内置了一些常见的如网站数据备份文件后缀名、常用日志文件后缀名等，若还需要自定义文件类型，则点击<新增>按钮，添加需要过滤的文件后缀即可，界面如下。

5.1.1.5. HTTP 异常检测

方法过滤：用于设置允许HTTP请求类型，即勾选的HTTP方法会被策略判定为异常，进行拦截，如下图所示。



HTTP头部字段检测：主要检测HTTP头部中的Referer、User-Agent、Host等字段是否存在SQL注入等攻击行为，可以根据实际情况是否对HTTP头部字段进行所有攻击检测或只检测SQL注入。

注：此功能要将[对象/安全策略模板/Web应用防护]中的对应模板防护类型的“sql注入”勾选启用才能生效，如下图所示。

例如，勾选“Host”字段后，当检测到HTTP头部字段存在SQL注入攻击，安全日志中标注的攻击类型依然是SQL注入攻击，拦截部分为HTTP数据包的头部Host字段。

溢出检测：主要防止HTTP的一些字段过长，导致溢出，如下图所示。

URL溢出检测：勾选启用URL溢出检测，设置最大长度，将会对URL的最大长度进行检测，防止造成缓冲区溢出。

POST实体溢出检测：勾选启用Post 实体溢出检测，设置Post数据的实体部分的最大长度，防止造成服务器接收数据溢出的错误。

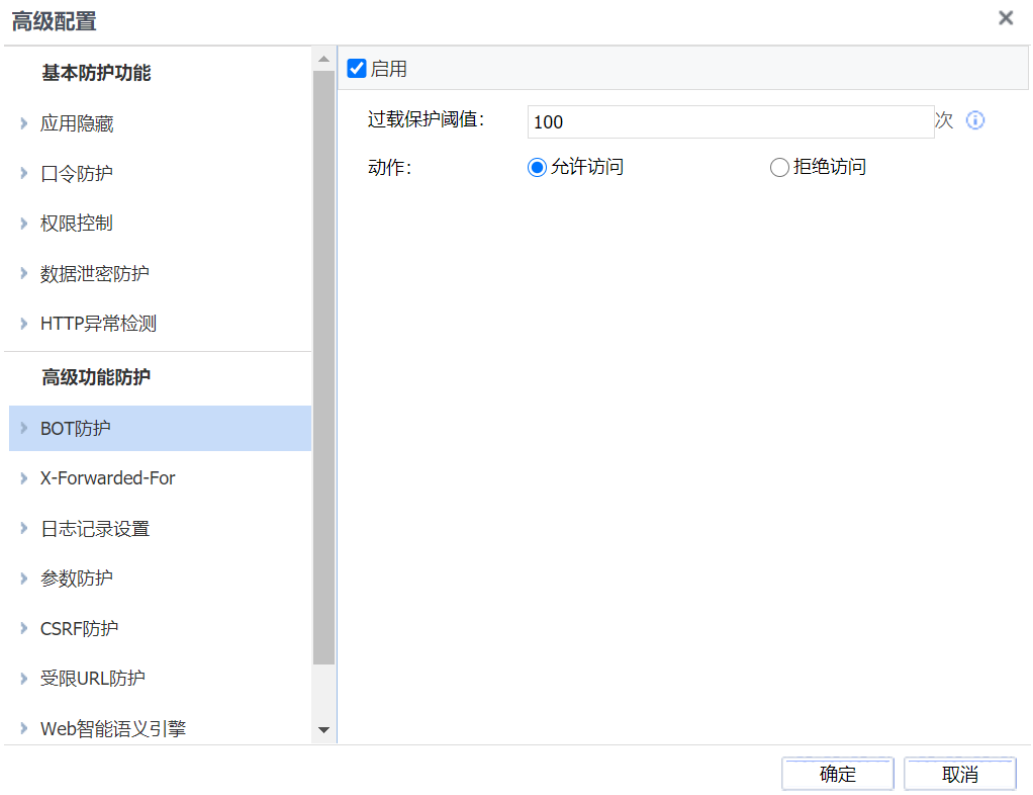
HTTP头部溢出检测：勾选启用HTTP头部溢出检测，点击<新增>按钮，设置需要检测HTTP头部中指定字段的最大长度，对该字段超出长度，进行检测。

range字段防护：勾选range字段防护，设置允许区间数，防止range字段数超出允许区间。

协议异常：主要是用于防护ASP和ASPX的页面中，请求多个参数被服务器错误处理，导致的复参攻击。同时，默认启用multipart头部字段长度的检测、Content-Type头部字段是否重复检测、请求方向chunk异常检测、请求方向charset头部字段是否重复检测和请求方向content-length异常检测。

5.1.1.6. Bot 防护

针对所有访问请求主动发其反向侦察探测代码来识别正常用户和自动扫描机器人，增强对漏洞扫描、爬虫等行为的识别拦截能力。该功能默认是不开启，如果开启Bot防护（需要先在防护配置勾选Bot防护和高级功能防护启用Bot防护），通过选择这个动作，可以拦截或者放过攻击，默认会记录日志，日志会上报云脑。



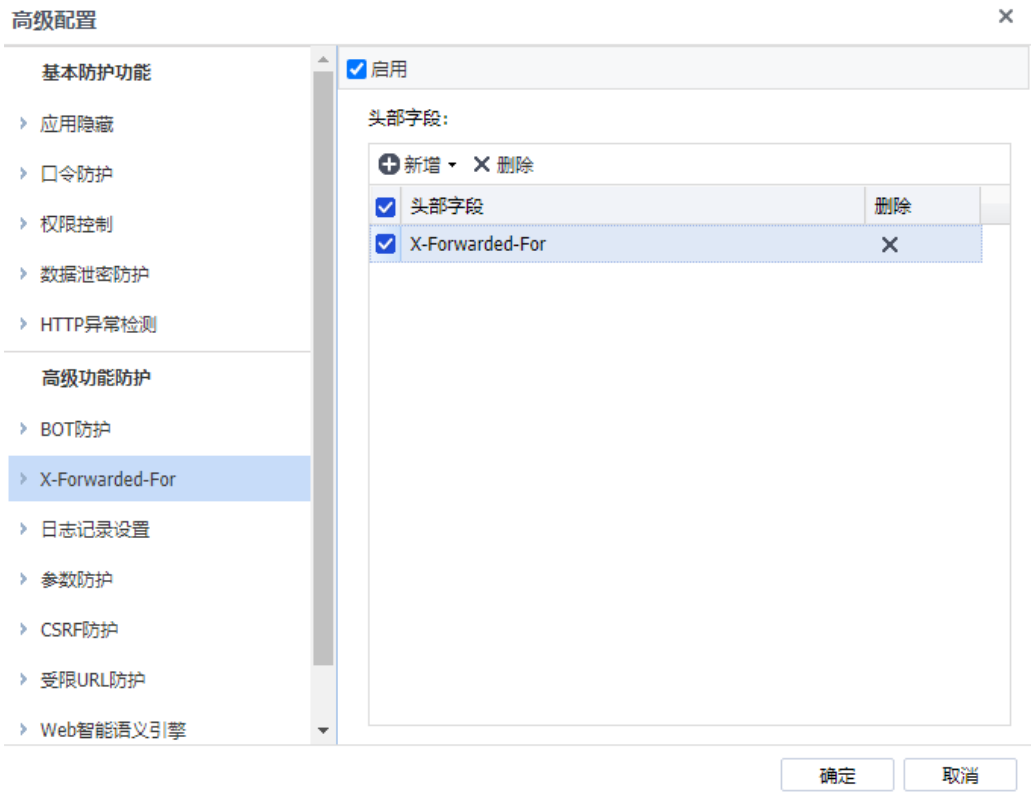
注意：

Bot 防护限制：Bot 防护仅支持 PC 端浏览器的业务、APP 浏览器的业务的防护；手机 APP 客户暂不支持，这类客户若配置 Bot 防护需根据 UA 来排除防止 APP 出现访问不了业务的问题。默认不开启该功能。

5.1.1.7. 高级功能防护

1. X-Forwarded-For

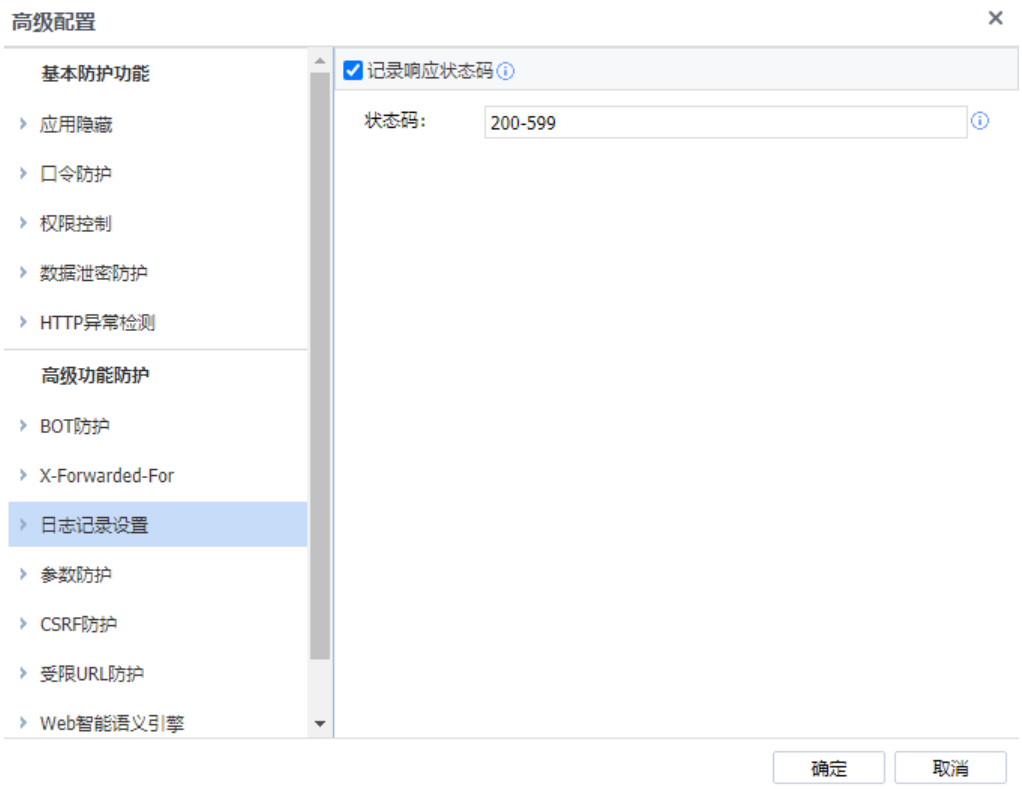
流量经过CDN或者代理等场景，一般都会在HTTP头部插入对应得X-Forwarded-For字段记录真实的源IP地址，以便服务器知道访问的真实IP。勾选启用，如下图所示。



头部字段：识别插入的HTTP头部字段，目前能够识别X-Forwarded-For、Cdn-Src-Ip和Clientip三种，也可以自定义进行配置。如下图所示。

日志记录设置

用于设置日志记录类型，页面如下。



状态码：配置范围为200-599，响应状态码记录状态码条件：

- 请求方向的攻击
- 检测到攻击动作是允许

注意：

如果外层启用开关关闭，但记录响应状态码处于勾选状态且引用当前模板的策略启用记录日志时，功能仍旧生效。

参数防护

自定义参数防护和主动防护功能类似，只是自定义相关参数，支持正则表达式匹配，表示满足设置相关正则表达式的条件后，匹配动作为拒绝。

CSRF防护

跨站伪造请求(Cross Site Request Forgery，CSRF)，也被称成为“one click attack”或者session riding，通常缩写为CSRF或者XSRF，是一种挟制终端用户在当前已登录的Web应用程序上执行非本意的操作的攻击方法。通过配置CSRF防护，可以有效防止该类攻击行为。配置页面如下。

通过配置需要进行防护的域名，已经新增需要防护的页面和允许访问的来源页面，保证跳转只能从允许访问的来源页面（Referer）来访问需要防护的页面（Target），达到组织CSRF攻击的目的。

受限URL防护

保护用户的关键资源不被非法客户端强制浏览。配置如下。

仅允许从www.sangfor.com.cn/bbs/index.html 访问www.sangfor.com.cn的域名主页，不允许通过其他方式的访问该域名。

Web智能语义引擎

通过智能语义引擎，对命令注入、PHP代码、JAVA代码、XEE攻击、Webshell上传、SQL注入、XSS攻击、后门扫描防护进行算法检测，不需要进行规则检测，从而提高检测率。如下图所示。

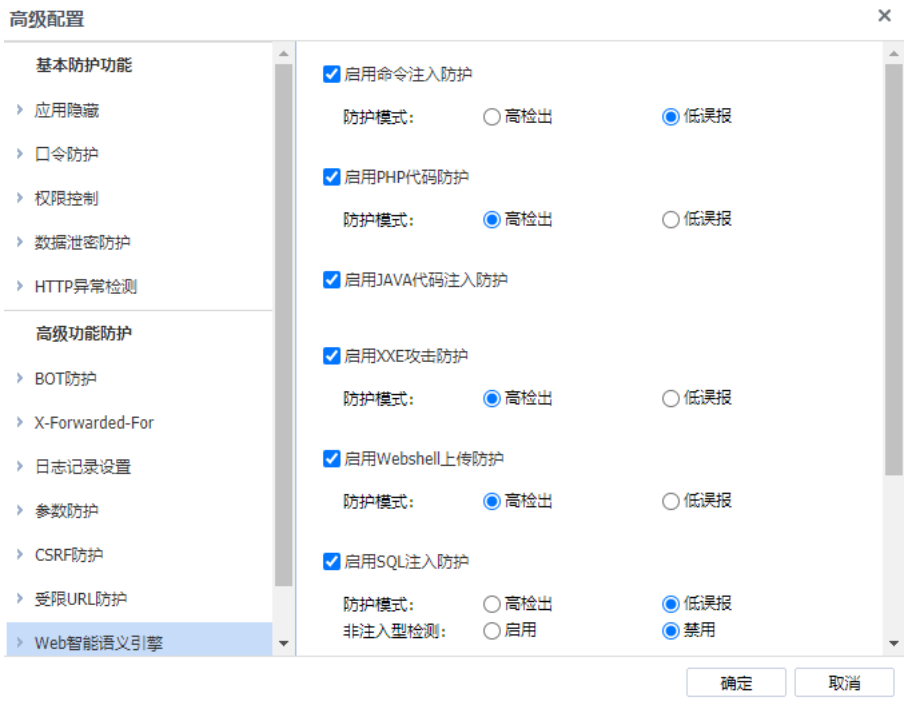
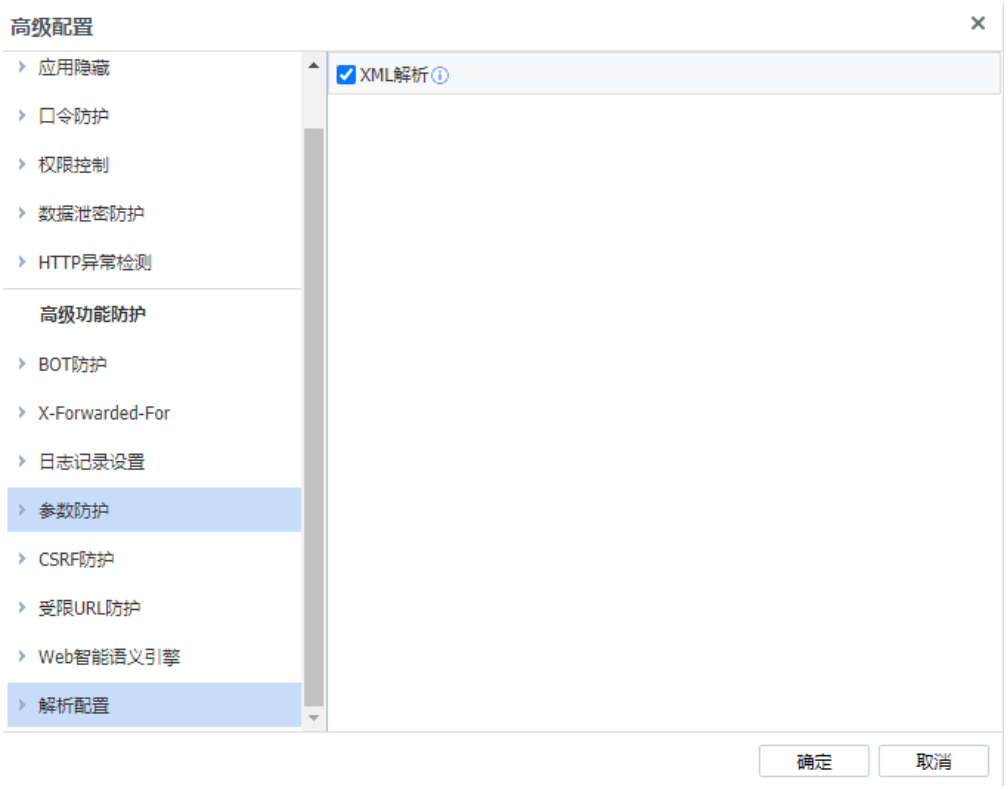


表7 Web智能语义引擎说明

引擎类型	说明
命令注入防护	提高命令注入攻击检测的安全效果，如果用户对安全性要求较高，可以接受一定的误报，建议选择高检出；如果用户对业务稳定性要求高，建议选择低误报。
PHP 代码注入防护	提升对未知漏洞进行 PHP 代码注入攻击的检测能力，减少对规则的依赖，如用户对业务稳定性要求较高，可选择低误报。
JAVA 代码注入防护	增加对更多 java 表达式语言的检测能力，减少漏报。
XXE 攻击防护	XXE 安全检测引擎，通过语法进行分析检测，减少漏报以及误报，提高云 WAF 拦截成功率，提高云 WAF 安全检测能力
Webshell 上传防护	减少因为缓冲区截断而导致的漏报，如果用户对安全性要求较高，能接受一定的误报，建议选择高检出如果用户对业务稳定性要求高，建议选择低误报。
SQL 注入防护	SQL 注入防护引擎，将改进云 WAF 的防御效果，增加抗绕过能力和降低误报率，该功能默认启用，并选择低误报和禁用非注入型检测，适用于 SQL 业务较多的场景，在 SQL 业务较少的场景下可选择高检出和启用非注入型检测。
XSS 攻击防护	XSS 攻击防护引擎可以增强对 XSS 攻击的检测能力，降低误报率，该功能默认启用，并选择低误报，适用于后台编辑前端页面较多的场景，在安全要求较高的场景下可以选择高检出。
后门扫描防护	后门扫描防护引擎可以增强对后门扫描攻击的检测能力，该功能默认启用，并选择低误报，在安全要求较高的场景下可以选择高检出。

解析配置

XML解析引擎检测功能，增强XML攻击检测识别。能够检测HTTP报文中的body部分，即通过XML协议传输包装的Webshell的一种攻击绕过手段。如下图所示。



5.1.1.8. 云端威胁防护

云端威胁防护配置：云端黑客IP防护，主要作用是联动云脑，拉取封锁IP库数据，进行临时封堵，提供快速有效的技术手段，及时阻断攻击行为，提升云WAF安全效果能力。勾选即开启云端黑客IP防护，如下图所示。

说明：

开启云端黑客 IP 防护需要云 WAF 连接到互联网，下发的黑客 IP 可在云端黑客 IP 进行查看。

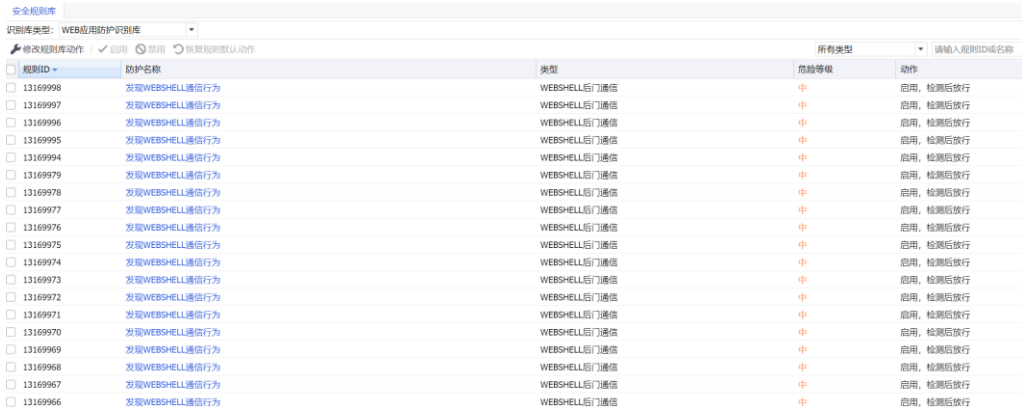
5.2. 安全防护规则库

5.2.1. 安全规则库

安全防护规则库主要提供给安全策略模板调用，该功能可以自定义规则，从而快速的响应，对攻击行为进行防护。

5.2.1.1. Web 应用防护特征库

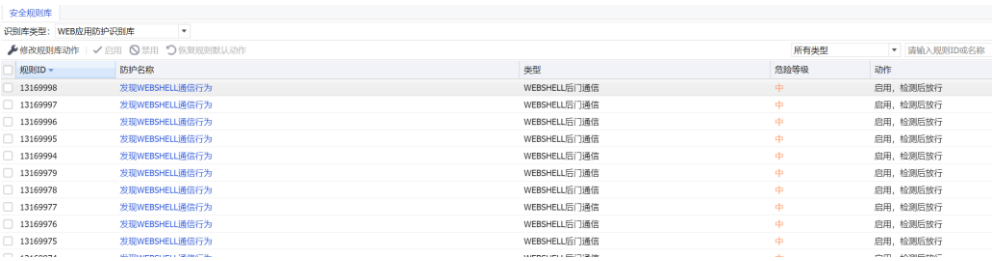
Web应用防护特征库内置了利用SQL注入、XSS攻击、网站木马、网站扫描、WebShell、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞等的应用层攻击包特征，当这些攻击包穿越设备时，可以根据用户设置拦截该攻击包，以保护服务器。界面如下。



点击<修改规则库动作>用于统一的修改Web应用防护规则。若选择默认（系统初始状态），则将保留系统自带的规则状态；若选择启用严格规则检测，并拦截，则对于所有防护规则的动作都将设置为启用，检测后拦截。对于危险等级为中的规则来说，系统默认的状态会放行的，启用严格检测后，危险等级所有的规则也将被拦截。如下图所示。

防护类型显示当前防护类型的规则库，点击下拉框，可以根据防护类型查看对应的规

则ID，防护名称显示该防护规则对应的名称，如下图所示。

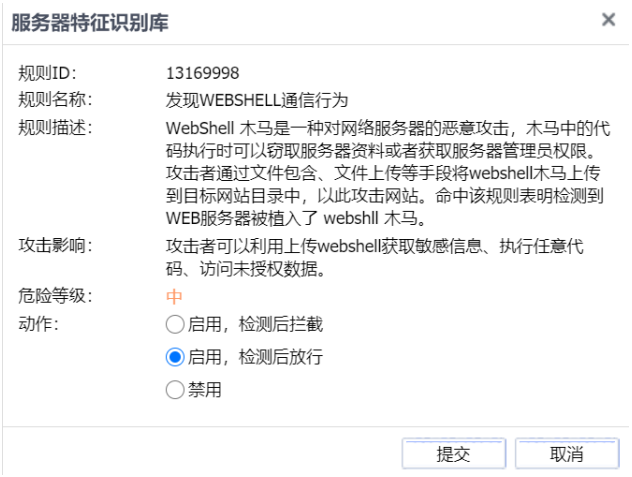


防护名称：显示该防护规则的名称。

类型：显示当前防护规则对应的防护类型，如SQL注入。

危险等级：描述此漏洞的危险等级，有高、中、低三个等级，等级越高的则危险程度越高。

动作：描述如果设备检测到该攻击行为时，设备所采取的动作，包括启用，检测拦截、启用，检测后放行、启用，与云分析引擎联动]、禁用四种。这个动作可以自定义，点击<防护名称>即可进入编辑页面，如下图所示。



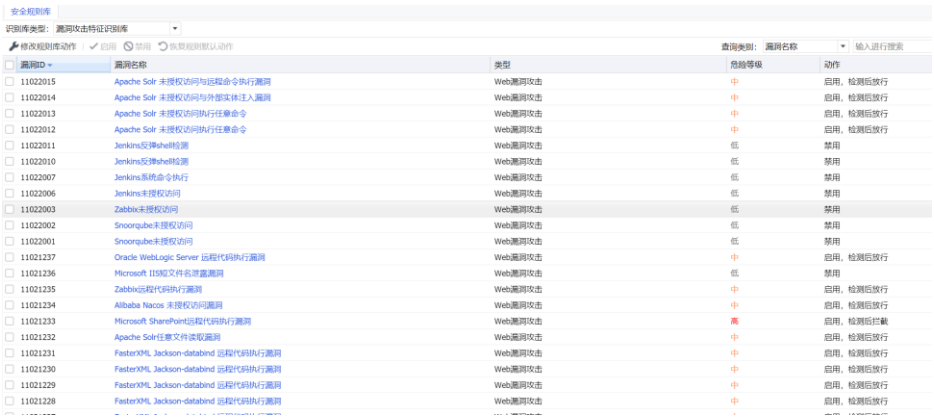
启用，检测后拦截：表示启用当前规则后当检测到此攻击行为时，拦截相应的数据包。

启用，检测后放行：表示启用当前规则，当检测到有攻击的行为时，只是记录日志，并不会拦截。

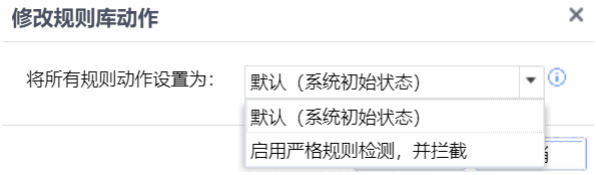
禁用：表示禁用当前规则，当规则禁用后，设备不会对该规则进行检测。

5.2.1.2. 漏洞攻击特征识别库

漏洞攻击特征识别库内置了利用系统、应用程序漏洞而进行攻击的攻击包特征，当这些攻击包穿越设备时，可以根据用户设置拦截该攻击包，以保护服务器，如下图所示。



修改规则库动作：用于统一的修改漏洞攻击特征识别规则。若选择默认（系统初始状态），则将保留系统自带的规则状态；若选择启用严格规则检测，并拦截，则对于所有识别规则的动作都将设置为“启用，检测后拦截”。对于危险等级为中的规则来说，系统默认的状态会放行的，启用严格检测后，危险等级所有的规则也将被拦截。



恢复规则默认动作：用于将修改过的规则动作全部恢复到默认状态。

漏洞攻击漏洞规则支持搜索功能，可以通过设置漏洞类别、查询类别，输入漏洞名称、ID等关键词进行搜索。

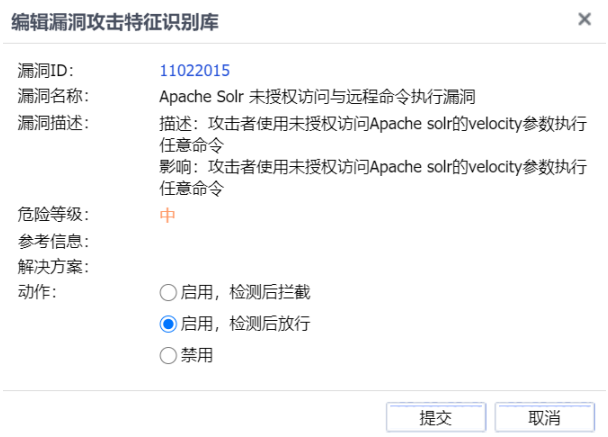
洞ID：显示当前漏洞的ID，主要作用是当服务器被某个漏洞攻击规则拦截了，可以到数据中心查看到漏洞ID，通过此处的漏洞ID查询，可以设置不拦截此规则。

洞名称：显示漏洞名称。

类型：显示当前漏洞的类型，如backdoor。

危险等级：描述漏洞的危险等级，有高、中、低三个等级，等级越高则危险程度越高。

动作：描述当存在利用该漏洞进行的攻击时，设备所采取的动作，包括启用、检测后拦截、启用，检测后放行、禁用。这个动作可以自定义，点击<漏洞名称>即可进入编辑页面，如下图所示。



启用，检测后拦截：表示启用当前规则，当有利用此漏洞进行攻击的行为时，拦截相应的数据包。

启用，检测后放行：表示启用当前规则，当有利用此漏洞进行攻击的行为时，只是记录日志，并不会拦截。

禁用：表示禁用当前规则，当规则禁用后，设备不会对该漏洞进行检测。

⚠ 注意：

漏洞特征库的放行和拦截属性出厂已经配置好，当需要修改某条规则的时候，编辑该条规则即可。

5.2.2. 自定义规则库

根据手工自定义规则库，能够及时的防护未发现的攻击行为。目前支持自定义Web应用防护规则库。

自定义Web应用防护规则库可以根据自定义规则来对新的Web攻击进行防护，从而解决突发的攻击行为。界面如下。

在自定义Web应用防护规则库页面，点击<新增>。

规则名称、描述、攻击影响可根据情况自己定义。

规则类型：可选自定义Web应用防护规则。

危险等级：可以选择高、中、低三个级别，用于定义规则的等级。

动作：可选择启用，检测后拦截、启用，检测后放行、禁用三类。

- 启用，检测后拦截：表示启用当前规则，当检测到此攻击的行为时，拦截相应的数据包。
- 启用，检测后放行：表示启用当前规则，当检测到有攻击的行为时，只是记录日志，并不会拦截。
- 禁用：表示禁用当前规则，当规则禁用后，设备不会对该规则进行检测。

字符串、正则表达式、匹配方向用于设置自定义规则内容，其中前两项可留空，留空则代表跳过此项匹配。

配置案例：

近日某Web服务器系统暴露出Apache漏洞，需要使用WAF临时把该漏洞封堵，从而防止不法分子利用该漏洞进行牟利。

步骤1.创建自定义规则，该漏洞主要是请求方向匹配Host:\s?[^q][^i][^c][^o][^n][^g][^1][^\x2e][^t][^o][^p][^\r\n]内容来进行漏洞利用，如下图所示。

步骤2. 在Web应用防护模板中，调用该规则，如下图所示。

步骤3. 在Web应用防护策略中调用防护模板。


WEB应用防护策略
新增
删除
启用
禁用
上移
下移
移动
刷新
高级设置
搜索
优先级
名称
启用状态
操作
1
官网
编辑 复制 删除
编辑WEB应用防护策略
常规
防御
检测响应
WEB应用防护
WAF
动作:
允许
拒绝
网站防篡改
需要网站管理员在服务器中安装Linux防篡改客户端 或 Windows防篡改客户端，客户端将防止黑客篡改文件系统。

6. 反向代理

云WAF支持反向代理功能，同时云WAF部署在客户端与服务器之间，对于用户而言，WAF就相当于目标服务器，即用户直接访问WAF就可以获得目标服务器的资源。同时，用户不需要知道目标服务器的地址，也无须在用户端作任何设定。反向代理服务器通常可作Web加速，即使用反向代理作为Web服务器的前置机来降低网络和服务器的负载，提高访问效率。

6.1. 虚拟服务

虚拟服务是当对外发布的Web应用服务，提供对外用户访问，并根据调用前置策略对站点实现不同的业务调度。创建虚拟服务，如下图所示。

名称：填写策略的名称。

描述：填写对应得描述信息。

服务类型：对外提供服务的类型，目前支持HTTP和HTTPS。

端口：对外提供HTTP或者HTTPS服务的端口，如果存在多个端口，需要分行填写。

默认节点池：调用对应的节点池，该节点池为当前置策略无法匹配时，默认调用该节点池。

SSL卸载策略：调用对应的SSL卸载策略，该功能只有选择HTTPS服务类型才支持。

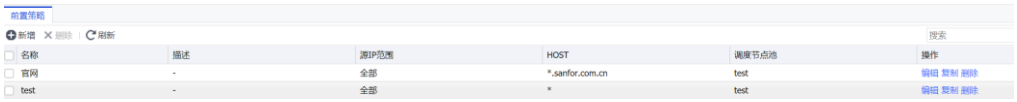
SSL加密策略：当SSL加密策略禁用时，为SSL卸载功能；当SSL加密策略启用时，为SSL解密功能。

前置策略：选择需要调用的前置策略。如果一个IP对应多个域名时，需要前置策略进行区分来调度到各个节点上。

x-forwarded-for：选择是否需要插入x-forwarded-for字段，可选择在末尾追加上一跳IP或者原封不动。

6.2. 前置策略

为了将特定用户的访问调度到指定节点池，我们可以配置前置策略对访问该虚拟服务的流量进行按需调度。如下图所示。



点击<新建>，创建前置策略，如下图所示。

名称：填写该前置策略的名称。

描述：填写对应得描述信息。

源IP范围：访问该站点的源IP，如果是发布到公网建议选择全部。

HOST：发布的域名/IP。

调度节点池：选择符合前置调度策略条件的用户访问某个虚拟服务时将会调度到的节点池。

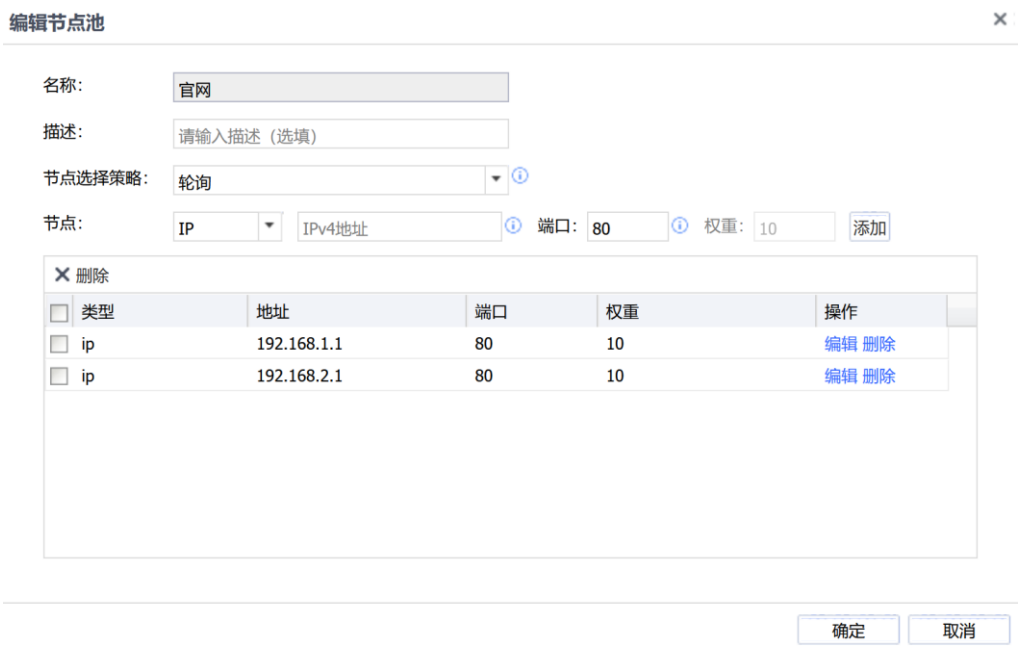
头部改写：可以对HTTP头部进行改写，如下图所示。

- **类型：**可以选择对请求头或者响应头进行 HTTP 头部修改。
- **动作：**选择添加或隐藏，对 HTTP 头部进行添加或者隐藏。
- **参数名：**填写对应得 HTTP 参数名称。
- **参数值：**选择 HTTP 头添加后，才能够加入对应的参数值。

6.3. 节点池

为了实现负载均衡，需要部署多个服务器节点同时发布业务，而节点池正好能满足将这些的服务器节点划到同一个资源池内去调度，使得客户端访问对应的服务时通过节点池的策略能够均衡地分布到这些服务器节点上面。如下图所示。

点击<新增>，创建节点池，如下图所示。



名称：填写对应节点的名称。

描述：填写对应节点的描述信息。

节点选择策略：配置节点选择策略类型，包括轮询、加权最少连接两种策略。

- **轮询：**表示数据轮询分发到各个节点。
- **加权最少连接：**表示根据权重选择（上下行流量之和/权重）最小的节点。

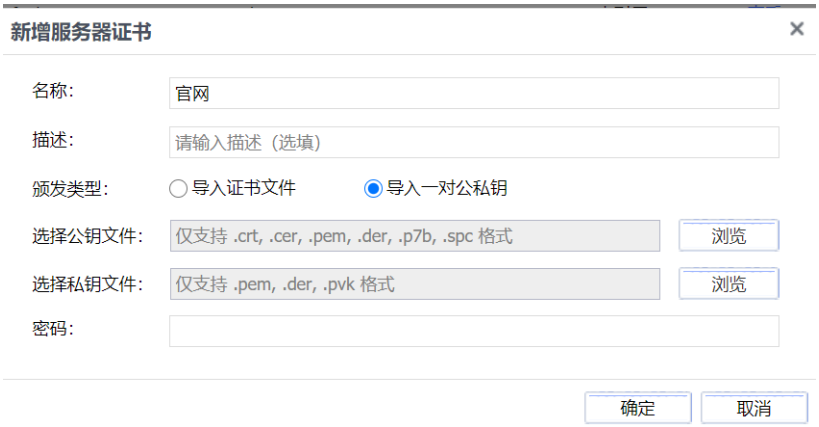
节点：配置调度的节点信息，包括IP、端口、权重（范围1-100，仅限于选择加权最少连接），配置后需要点击后面的<添加>按钮将节点添加到节点池的调度里面。

6.4. SSL 策略

SSL策略功能，主要是对HTTPS服务进行加解密，使云WAF能够对业务进行安全防护。而HTTPS是使用公钥、CA证书（可选）和私钥对流量进行加密，因此需要解密HTTPS流量需要导入对应的证书信息。

点击<服务器证书>，导入对应的网站HTTPS证书，如下图所示。

点击<新增>，创建服务器证书，如下图所示。



新增SSL卸载策略，如下图所示。

名称：填写对应的SSL卸载策略名称。

描述：填写描述信息。

服务器名称SNI：填写服务器名称信息。

服务器证书：选择该站点的HTTPS服务器的证书。

启用协议：不同的客户端浏览器支持的协议类型版本不一样，如浏览器版本较低的使用协议可能是TLS1.0，为适配所有客户端的浏览器协议类型，建议全部勾选。

加密算法：每个套件都以“SSL”开头，紧跟着的是密钥交换算法。用“With”这个词把密钥交换算法、加密算法、散列算法分开，例如：SSL_DHE_RSA_WITH_DES_CBC_SHA，表示把DHE_RSA(带有RSA数字签名的

暂时Diffie-HellMan)定义为密钥交换算法；把DES_CBC定义为加密算法；把SHA定义为散列算法。具体Web服务器支持的算法需要与WAF的一致或者WAF比Web服务器支持的多，从而保证WAF的算法包含完Web服务器支持的算法，否则WAF无法加解密对应的数据包。未勾选的算法可能存在已知漏洞，如果WAF上线后存在某些页面无法打开，可以增加算法的方式来解决。默认算法已经包含大多数服务器使用的算法，如无其他需求，保持默认即可。

7. 策略

策略作为设备的主要功能模块，提供完整的安全防御体系，确保安全防护不存在短板，针对经过设备的数据包根据策略进行检测，发现攻击行为进行告警和记录日志。

7.1. 安全策略

安全策略是云WAF的核心功能之一，能够对经过云WAF的流量进行安全检测。安全策略主要包括Web应用防护策略和业务模型学习监督。

7.1.1. Web 应用防护策略

安全防护策略是统一配置安全功能的入口，在这里可配置Web应用防护和防篡改安全功能。

可以对安全防护策略进行新增、删除、启用、禁用、上移、下移、移动、刷新、高级设置和筛选操作。

WAF产品均是以域名为防护维度，保护客户的Web应用的业务安全。从用户角度来看WAF专业化程度低，所以实现域名精细化管理。需要虚拟策略配置完成后才能调用该域名进行精细化管控。

点击<新增>，创建Web应用防护策略，如下图所示。

策略名称：定义策略名称。

描述：定义描述信息。

状态：定义策略是否启用。

目的域名：选择对应防护的域名，进行精细化防护。该域名需要完成虚拟服务的创建才能够识别到。

业务访问场景：提前明确访问过程中，是否存在源地址转换或者CDN等代理的场景，共两个选项,“访问源未经过源地址转换或CDN”和“访问源经过源地址转换或CDN”。

访问源未经过源地址转换或CDN：即流量到达WAF时，源IP为客户端的公网IP。

访问源经过源地址转换或CDN：即流量到达WAF时，源IP全部为CDN地址或者经过SNAT转换后的地址，从而无法辨别具体的客户端公网IP。

说明：

CDN（内容分发网络）是构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。如果边缘服务器无该服务内容，则会使用本地的 IP 向中心服务器进行资源请求，从而边缘服务器起到一个代理的作用。

点击<下一步>，进入防御配置。如下图所示。

Web应用防护策略：选择是否启用Web应用防护策略，且选中引用相关的Web应用防护模板。专门针对Web服务器设计的防攻击策略，可以防止系统命令注入、SQL注入、XSS攻击等各种针对Web应用的攻击和泄密行为。

网站防篡改：对服务器进行文件系统防护，防止被篡改时。需要在服务器上安装一个防护客户端，该客户端通过设置地址与云WAF通信、输入防护的网站目录、允许修改防护文件的应用程序等保护服务器文件系统避免被黑客修改。防篡改客户端与云WAF使用端口为TCP/9000，如发现存在修改行为则会上报给云WAF进行告警。

说明：

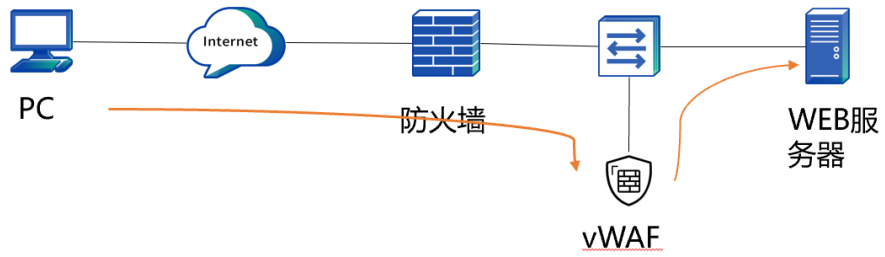
1、windows 客户端适用于 Windows 2003（32/64bits）、Windows 2008（32/64bits）、Windows 2012（32/64bits）。
2、linux 客户端适用于 CentOS 5/6/7 64bit、Debian 6/7 64bit、Ubuntu 10.04-14.4 64bit、RHEL 5/6/7 64bit。
3、防篡改客户端不支持 Windows 2016 及以上，如有需要可以使用 EDR 进行防护。

点击<下一步>，进入检测响应。如下图所示。

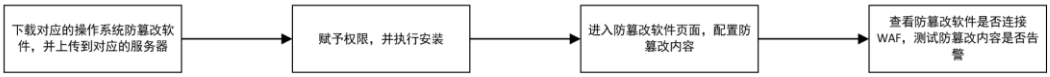
记录日志：勾选记录日志，触发攻击行为会记录相应日志到安全日志中。

防篡改配置案例

某企业Web服务器对互联网提供服务，经常遭受来自互联网的恶意攻击，为了防止黑客攻击成功篡改网站，需要对服务器的Web页面进行安全防护。

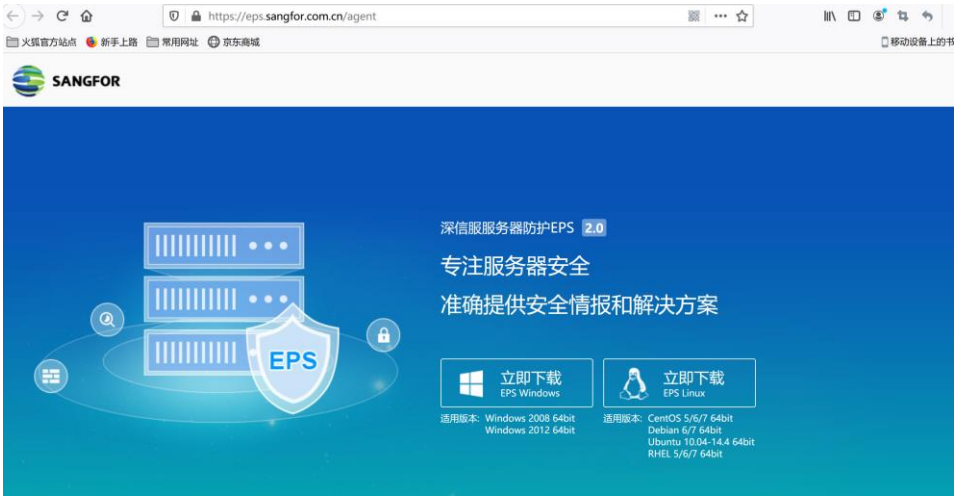


配置思路：

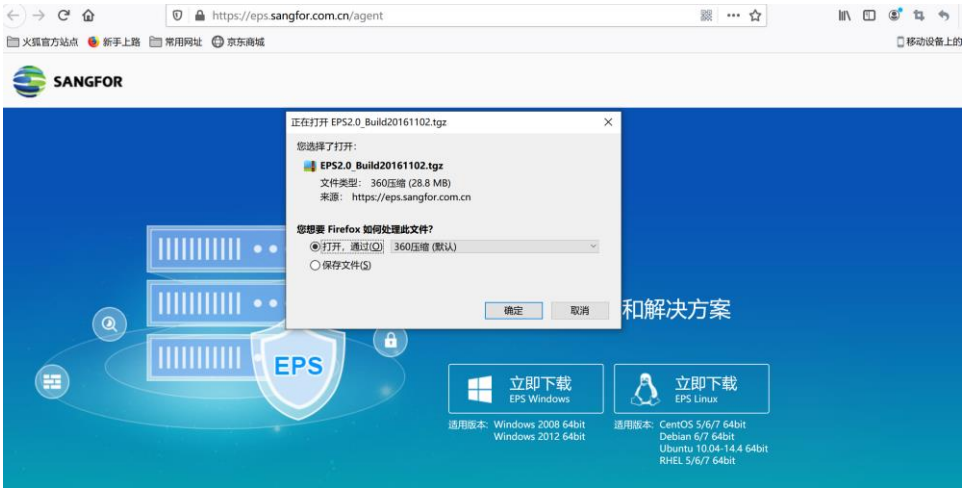


步骤1.在安全防护策略中，开启防篡改策略，如下图所示。

步骤2.（根据实际操作系统选择）点击<Linux防篡改客户端>，跳转到下载防篡改客户端页面（https://eps.sangfor.com.cn/agent），如下图所示。



步骤3.点击<立即下载>，下载对应得客户端，并拷贝到服务器上，如下图所示。



将下载的数据包上传到服务器上，使用ls命令查看是否上传成功。

```
af@debian:~$
af@debian:~$
af@debian:~$
af@debian:~$ cd /tmp/
af@debian:/tmp$ ls
EPS2.0_Build20161102.tgz  ssh-grxav12180
af@debian:/tmp$
```

步骤4.在Linux服务器，使用root账户下解压EPS2.0_linux.tgz（解包tar -zxf [路径/文件名]），如下图所示。

```
root@debian:/tmp#
root@debian:/tmp#
root@debian:/tmp# tar -zxf EPS2.0_Build20161102.tgz
root@debian:/tmp# LS
bash: LS: command not found
root@debian:/tmp# ls
agent_installer.bin  EPS2.0_Build20161102.tgz  ssh-grxav12180
root@debian:/tmp#
```

步骤5.赋予文件可以执行权限，并运行agent_install.bin脚本进行安装，如下图所示。

```
root@debian:/tmp#
root@debian:/tmp# chmod 777 agent_installer.bin          赋予可执行文件
root@debian:/tmp# ./agent_installer.bin /home/eps_test/  执行安装到指定目录下
eps agent is installing on x86 machines
extract eps_base.tgz
extract eps_packman.tgz
extract eps_sys.tgz
extract sfguard.tgz
/home/eps_test/ install success
eps start success
root@debian:/tmp#
root@debian:/tmp#
```

步骤6.查看安装目录下的文件，如下图所示。

```
root@debian:/tmp# cd /home/eps_test/
root@debian:/home/eps_test# ls
agent_scripts  bin  config  lib  lmodules  lualibs  packages  services  var
root@debian:/home/eps_test#
```

步骤7.进入到安装目录的bin下，执行. /sfgconfig命令进入操作界面，如下图所示开启防篡改相关功能。

```
root@debian:/home/eps_test#
root@debian:/home/eps_test# cd bin/
root@debian:/home/eps_test/bin# ls
agent_list              epsxtest          sfgconfig
agent_list.l            get_appversion    sfginject
cpulimit                ipc_probe         sfginject.bin
enable_sshd_execmem     ipc_probe.l       sfglogs
eps_app                 ipc_proxy         sfgpromote
eps_monitor             lloader           sfgpromote.bashrc
eps_services            luadbg            sfgpromote.l
eps_services_check.sh   patchelf
eps_uninstall.sh        resmon_export.sh
root@debian:/home/eps_test/bin# ./sfgconfig
```

步骤8.执行后，打开防篡改页面，进行配置，如下图所示。

[x]Enable SFGuard systsm 启动网站篡改防护系统。

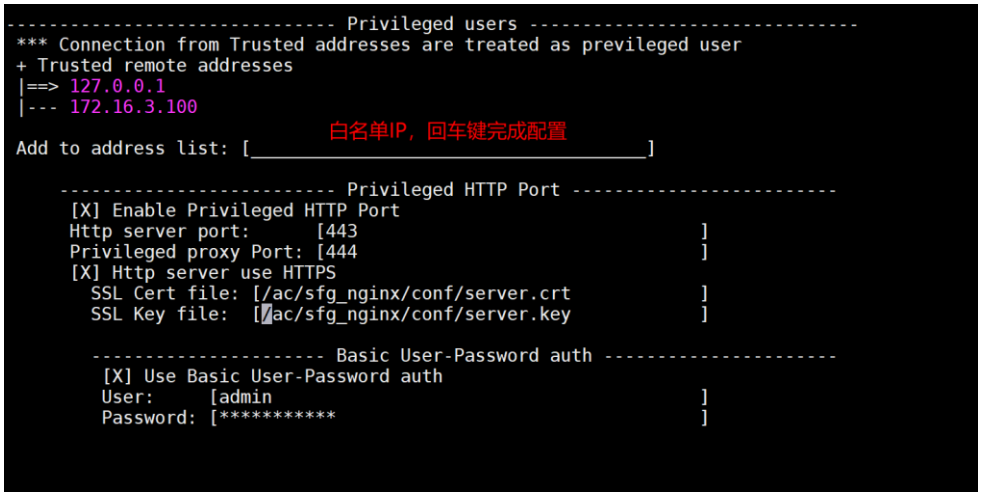
[x]log to Sangfor NG云WAF device 发送日志到深信服云WAF设备。

Sangfor NG云WAF address：[192.168.1.1] 云WAF设备IP地址，仅支持IPv4。

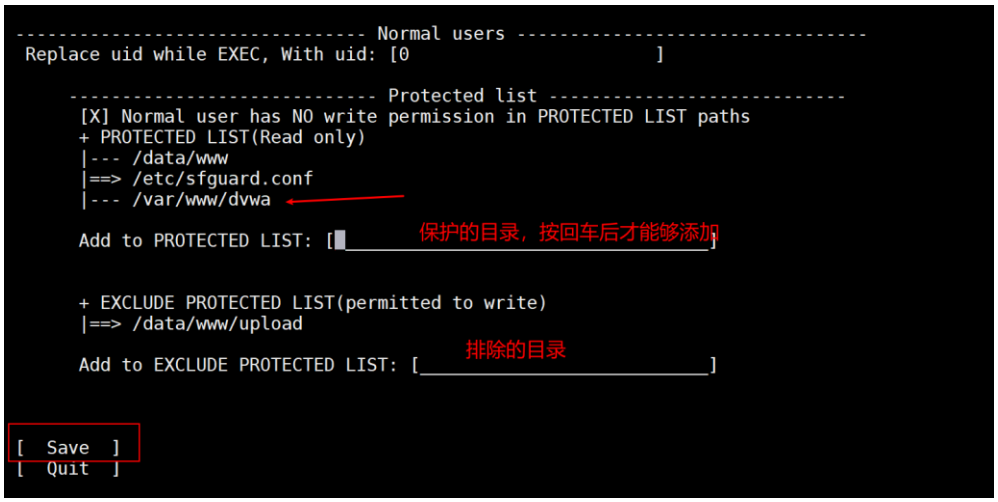
Guard Policy Name:在云WAF设备上的策略防篡改策略名称，两边保持一致。这些都是第一次让防篡改客户端和防火墙联动的必要条件，都要填上。

步骤9.（可选）配置进程白名单，使进程可以对文件进行修改，如下图所示。

步骤10.（可选/建议使用）IP地址白名单，白名单的IP操作直接绕过防篡改软件过滤。



步骤11.设置防护目录列表，并保存配置，如下图所示。

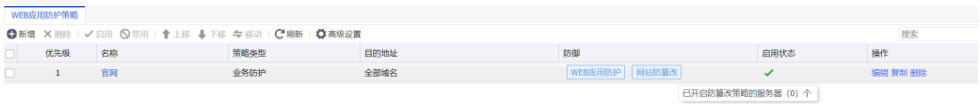


Add to protected LIST： 此目录下的文件将被防篡改保护。

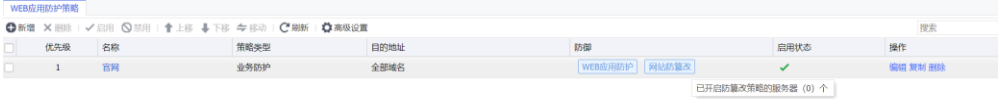
Add to EXCLUDE BLACK LIST:此目录下的文件将被防篡改排除保护。

先save，再quit退出。

步骤12.云WAF创建业务防护策略，名称与防篡改客户端一致，如下图所示。



步骤13.连接成功后，把鼠标放到网站防篡改，可以看到连接的服务器，如下图所示。



步骤14.连接成功后，在保护目录下进行修改文件，不在白名单内的IP或者进程会禁止修改，如下图所示。

```
root@debian:~#
root@debian:~#
root@debian:~# cd /var/www/DVWA/
root@debian:/var/www/DVWA# mkdir test
mkdir: 无法创建目录"test": 权限不够
root@debian:/var/www/DVWA# touch test.text
touch: 无法创建"test.text": 权限不够
root@debian:/var/www/DVWA#
```

步骤15.查看云WAF上的安全日志，如下图所示。

⚠ 注意 ：

1、因为防篡改需要对系统调用进行拦截，功能安装过程中需要使用 root 权限用户。

2、在防篡改功能开启前已经建立的会话或者连接，防篡改功能不会生效。新的会话或者连接才生效。

3、更改防篡改配置以后，重新建立新的会话来连接和操作，中间防篡改注入配置可能会有一定生效时间。

4、已经被防篡改保护的会话或者连接，在防篡改进程停止的情况依然会生效，如果要关闭防篡改功能，请通过配置开关停掉防篡改功能。

5、防篡改 Agent 的安装目录建议安装到/usr/local 或者/opt 目录下。

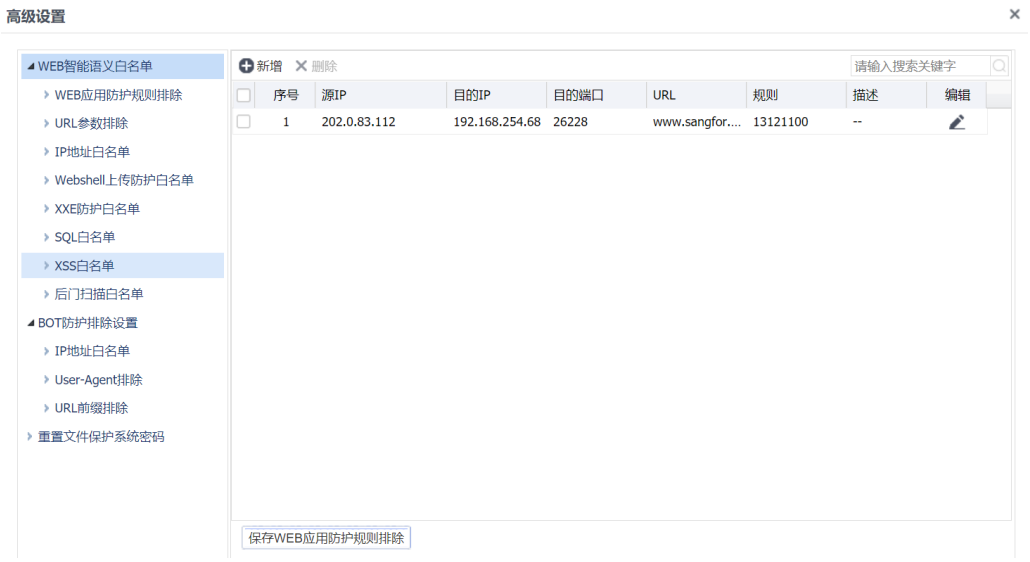
6、Agent 自身的 bypass 机制，当客户环境中内存系统资源超过 70%时，功能不生效。

7、防篡改配置界面不支持中文。

7.1.1.1. 高级设置

高级配置功能主要是对于影响业务或者误报的规则进行添加例外。添加例外后的规则不在进行检测且不告警。添加例外的规则包括Web智能语义、Bot防护排除设置和重置文件保护系统密码。

点击<高级设置>，弹出高级设置页面，如下图所示。



Web智能语义白名单：

可以对Web检测中存在误报的规则添加例外，包括Web应用防护规则、URL参数、IP地址、Webshell上传防护、XXE防护、SQL、XSS和后门扫描等添加例外，从而减少误报的发生。

Web应用防护规则排查：对Web检测出的误报规则进行排除，从而减少业务受到影响。点击<新增>，弹出Web应用防护规则排除设置。如下图所示。

源：定义源IP，可以是指定IP。

目的：定义目的IP。

目的端口：定义目的端口。

URL：定义排除的URL。

描述：定义描述信息。

规则ID：定义规则ID。

规则类型：定义规则类型，对某一类规则添加例外。

点击<确定>，提交配置。

点击<保存Web应用防护规则排除>，对云WAF规则排除设置进行保存。

URL参数排除：可以添加URL参数进行排除。

点击<新增>，弹出URL参数排除设置界面。如下图所示。

URL：定义URL。

参数：定义参数信息。点击新增，输入参数名称和参数特征串，如下图所示。

参数名称：填写URL的参数名称；

参数特征串：使用正则表达匹配参数的特征，从而达到模糊匹配的效果。

点击<确定>，提交配置。

点击<URL参数排除>，对URL参数排除设置进行保存。

IP地址白名单：可对IP地址进行排除。如下图所示。

点击<下载示例文件>，可下载模板文件，按格式填入要排除的IP，最后导入。

点击<保存IP地址白名单>，对IP地址白名单设置进行保存。

Webshell上传防护白名单：针对Web智能引擎检测出来的Webshell上传出现误报时，可以对Webshell上传的防护加入白名单，从而减少误报造成的影响。

点击<新增>，跳转到安全日志界面，需要在安全日志后添加例外，可加入到白名单中。

XXE防护白名单：针对Web智能引擎检测出来的XEE出现误报时，对XXE的防护添加到对应的白名单中，如下图所示。

输入对应的域名即可，点击<保存>生效。

SQL白名单：针对Web智能引擎检测出来的SQL语义出现误报时，可以对SQL注入的防护加入白名单，从而减少误报造成的影响。

点击<新增>，跳转到安全日志界面，需要在安全日志后添加例外，可加入到白名单中。

添加例外，如下图所示。

XSS白名单：针对Web智能引擎检测出来的XSS语义出现误报时，可以对XSS注入的防护加入白名单，从而减少误报造成的影响。

点击<新增>，跳转到安全日志界面，需要在安全日志后添加例外，可加入到白名单中。

添加例外，如下图所示。

后门扫描白名单：针对Web智能引擎检测出来的后门扫描出现误报时，可以对后门扫描加入白名单，从而减少误报造成的影响。

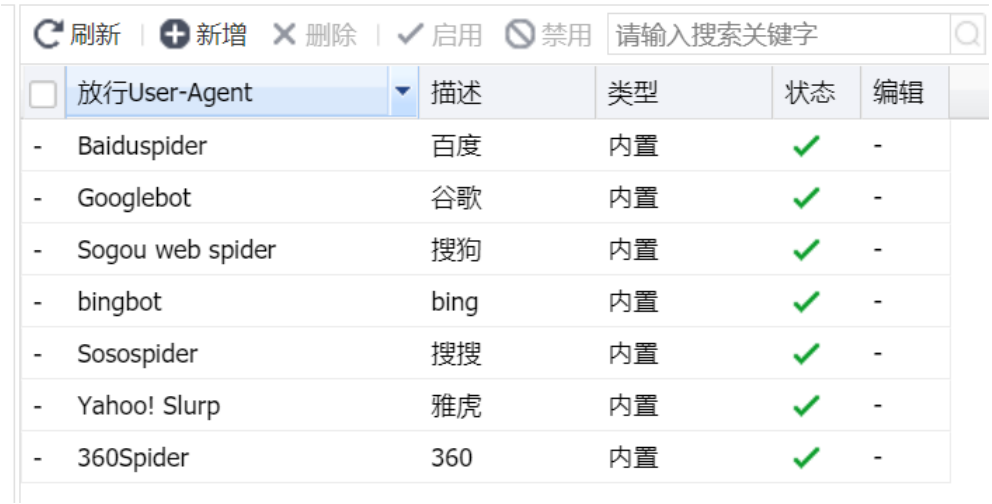
点击<新增>，跳转到安全日志界面，需要在安全日志后添加例外，可加入到白名单中。

添加例外，如下图所示。

Bot防护排除配置

IP地址白名单：对触发误报的IP添加到白名单中。

User-Agent排除：对匹配上HTTP头部user-agent的内容进行添加例外，从而减少误报。如下图所示。

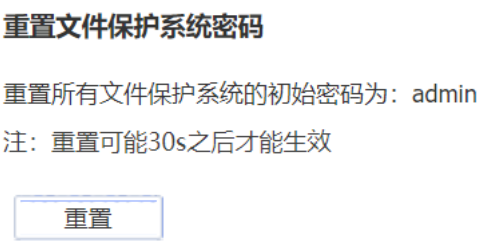


URL前缀排除：对匹配上的URL前缀进行排除例外，从而不进行不检测。

重置文件保护系统密码：

开启防篡改功能后，忘记了服务器端配置的密码，则可以重置所有文件保护系统的初

始密码为：admin，重置可能30s之后才能生效。界面如下。



点击<重置>，弹出确认重置页面。如下图所示。

点击<确定>，进行重置，点击<取消>，不进行重置。

7.1.2. 业务模型学习监督

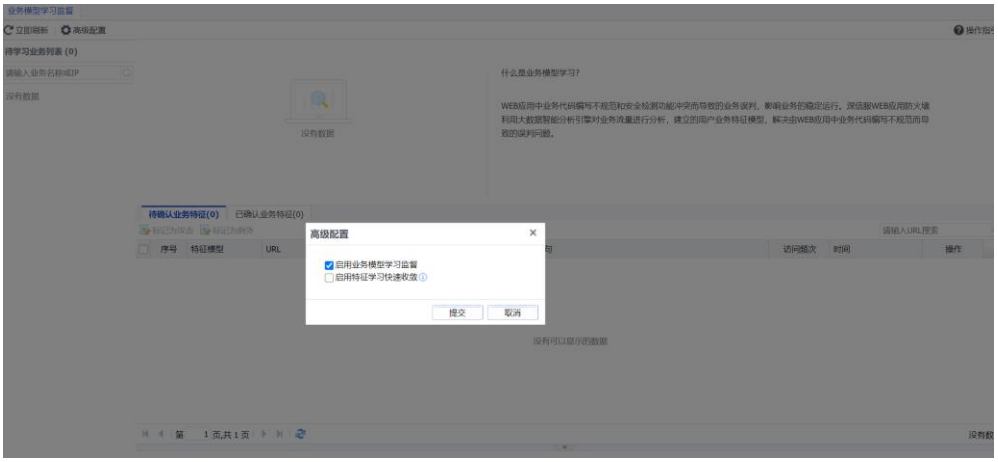
Web应用中业务代码编写不规范和安全检测功能冲突而导致的业务误判，影响业务的稳定运行。深信服防火墙利用大数据智能分析引擎对业务流量进行分析，建立的用户业务特征模型，解决由Web应用中业务代码编写不规范而导致的误判问题。

原理：

业务模型学习使用AI半自动化学习算法(部分需要人工参与)解决Web业务代码编写不规范导致业务误判问题，能够将Web应用安全策略开启防御模式，保障业务系统的安全与稳定运行。

AI半自动化学习算法对Web业务访问的流量进行分析与学习，学习Web业务系统特征；然后将基于攻击特征和业务特征的检测方式进行融合，解决Web业务代码编写不规范导致的误判问题。对于AI学习算法无法自动判别的特征，通过人工进行判别与标记；该学习方法需要针对业务系统访问流量持续学习一段时间，直到业务系统的特征全部学习完成，才能将对应业务的Web应用防护策略开启防御。

点击<高级配置>，勾选启用业务学习模型，则开启业务模型学习的功能，如下图所示。



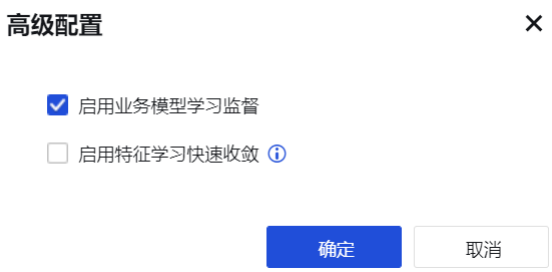
启用业务模型学习监督：开启业务模型学习功能；

启用特征学习快速收殮：针对特定URL的特征不断变化时，加快特征学习速度，启用该功能可能会引起漏判风险，需谨慎使用。

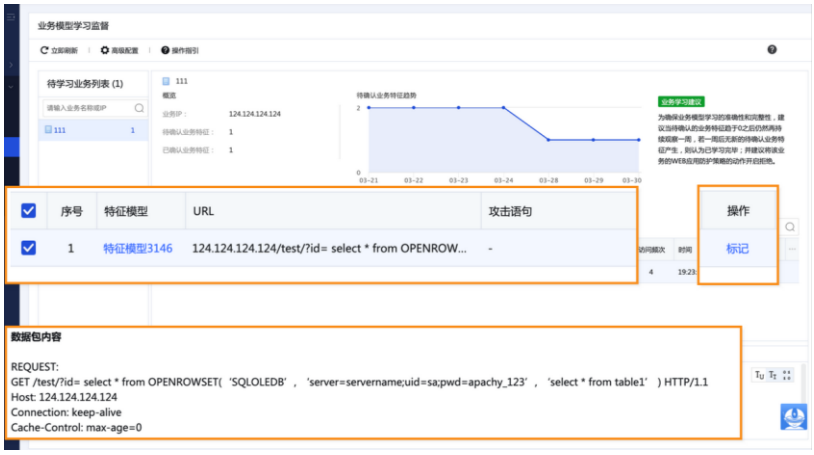
配置案例

某企业网络中上线一台云WAF，作为应用服务器的防护。但是上线后，由于业务编码不规范等问题，出现较多的误报信息，导致无法开启阻断的功能。

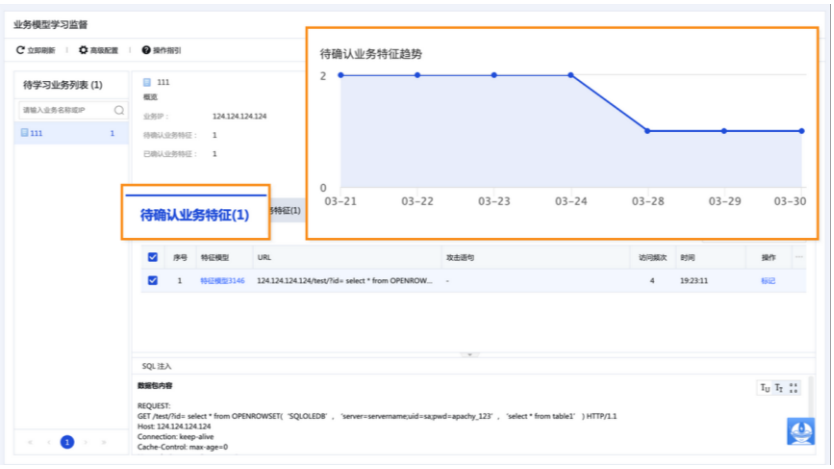
步骤1. 开启业务模型学习监督功能，对业务编码不规范进行学习，如下图所示。



步骤2. 查看业务特征对应的原始数据包内容(高亮部分为特征)，判别该特征是正常的业务访问特征还是攻击特征，并对其进行标记。



步骤3. 当业务待确认特征趋势趋于0，且连续两周内无新的待确认特征产生，则表明该业务系统的业务特征已学习完毕，建议将该业务系统的Web应用防护策略的动作开启拒绝。



步骤4. 在[策略/安全策略/Web应用防护策略]页面找到对应业务的策略，然后在编辑业务防护策略弹窗中，点击下一步，到防御页面，将Web应用防护的动作配置为拒绝。

8. 系统

系统主要用于设置系统功能以及参数方面的设置，包括安全能力更新、通用配置、排障、管理员账号和系统维护等功能模块。

8.1. 通用配置

通用配置包括控制台配置、网络参数、邮件服务器、系统时间、授权管理和隐私设置。

8.1.1. 系统时间

系统时间用于设置设备的系统时间。可以直接在页面上修改时间，也可以选择与[时间服务器]进行同步。

日期和时间设置用于查看系统的当前时间，也可以在此处手动设置系统时间。点击<获取本地时间>，则设备的系统时间会和登录控制面板的计算机时间一致，点击<获取系统时间>，可实时刷新设备系统本身的时间。

设备的系统时间也可以设置成和时间服务器同步，在[时区设置]中选择设备所在的时区，在[与Internet时间服务器同步]中设置公网的时间服务器地址，则设备会自动与此时间服务器的时间进行同步。

⚠ 注意：

修改系统时间将导致 Web 服务器重启，保存后需要重新登录控制台

8.1.2. 网络参数

网络参数用于配置全局网络相关参数说明。

网络参数

SSH端口：用于设置进入后台的端口，默认为22345。

业务安全页面显示模式：设置业务安全的显示模式，有缓存模式和实时模式可供选择。如果选择缓存模式这优先调用缓存的内容，则显示的内容速度更快，更新速度慢。而实时模式则显示内容速度慢，会消耗较多的设备资源。

BASE64解码：设定Web应用防护是否对base64数据进行安全检查

异常BASE64检测：设定Web应用防护是否允许对不合规范的BASE64数据进行安全检查。

body严格识别：设定根据body内容来判定数据类型。

8.1.3. 控制台配置

[控制面板配置]包括WebUI选项和认证参数设置。

WebUI选项下可以设定设备名称、WebUI端口、控制超时，配置页面如下所示。

语言设置：只支持简体中文，不支持切换到英文。

设备名称：可以设置设备的显示名称。

Web UI端口：用于设置登陆控制台的端口，默认是TCP 4431端口。

控制超时(m)：设置的是控制台超时时间，如果管理员在设定时间内控制面板无操作，系统会自动断开连接。

智能客服：设置在控制台界面是否开启智能客户小机器人的选项。

动态验证码：设置在控制台登录时是否开启输入动态验证码的选项。

最大并发管理数：设置最大允许多少个人同时登录设备控制台。

单用户限制：设置允许从多少个不同的地址使用同一管理员账号登录设备控制台。

登录失败重试：设置同一管理员账号允许的登录失败次数。

点击<提交>保存配置生效。

8.1.4. 邮件服务器

[邮件服务器]用于设置设备发送告警邮件的时候使用的SMTP服务器信息。

发件人邮箱：填写设备发送告警邮件的时候使用的邮箱，例如test@domain.com。

SMTP邮件服务器：填写发件箱对应的SMTP邮件服务器的域名或者IP地址。如SMTP邮件服务器需要验证用户名和密码则勾选“需要验证服务器用户名和密码”。

SSL：勾选则采用SSL协议进行传输。

端口：定义SMTP服务器端口。

SMTP邮件服务器身份验证：填写发件人邮箱的用户名和密码。

- 用户名：可填邮箱地址，也可填用户名。
- 密码：如果发件人邮箱已启用第三方客户端授权码，则密码处填写授权码。

填写了地址后点击<发送测试邮件>可以检测是否可以发送成功。

点击<测试>，发送测试邮件成功后，可以到测试的邮箱地址查看是否收到测试邮件。

使用深信服提供的邮箱：使用深信服科技提供的发件人邮箱和SMTP邮件服务器，邮件默认使用SSL加密，端口为465（SMTPS）。

⚠ 注意：

网站篡改防护设置了篡改后邮件通知管理员，会使用此处设置的 SMTP 服务器信息发送邮件。设置的邮件告警，会使用此处设置的 SMTP 服务器信息发送邮件。

操作步骤

步骤1. 例如配置QQ邮箱服务器，需要在[设置/账号]找到服务器配置方式，确保SMTP已开启。根据需求点击<如何使用 Foxmail 等软件收发邮件？>去获取STMP服务器地址和端口。

步骤2. 点击<生成授权码>，跳转验证码发送页面，使用绑定邮箱的手机号发送短信到指定的号码，手机上发送成功，再点击<我已发送>。

步骤3. 页面弹出生成授权码。

步骤4. 进入[邮件服务器]配置页面。填写刚才配置的邮箱地址、SMTP服务器地址、服务器端口。STMP服务器验证填写的用户名与发件邮箱一致，密码为授权码。

步骤5. 点击<发送测试邮件>，输入能正常接收邮件的邮箱地址进行测试，如下图所示。

步骤6. 发送成功后，发送测试地址的邮箱收到测试邮件，说明配置的发送邮件服务器能正常发送邮件。点击<保存>邮件通知服务器配置完成。测试邮件如下图所示。

8.1.5. 授权管理

授权管理包括设备基础信息、安全功能模块开通及安全能力升级序列号、云端订阅服务序列号和软件升级和维保服务，如下图所示。

设备基础信息：描述了设备从基本概况，其中网关序号是云WAF设备软件的唯一标识升级和激活都需要提供。

安全功能模块开通及安全能力升级序列号：用于启动设备各安全功能模块，其中包括Web服务器防护功能、Web应用防护功能。

云端订阅服务序列号：与云端联动，实现更新云WAF的防护能力同时，辅助云WAF对未知、高级威胁等进行有效检测和抵御。其中云脑-云智主要是对云WAF的各功能模块规则进行更新。

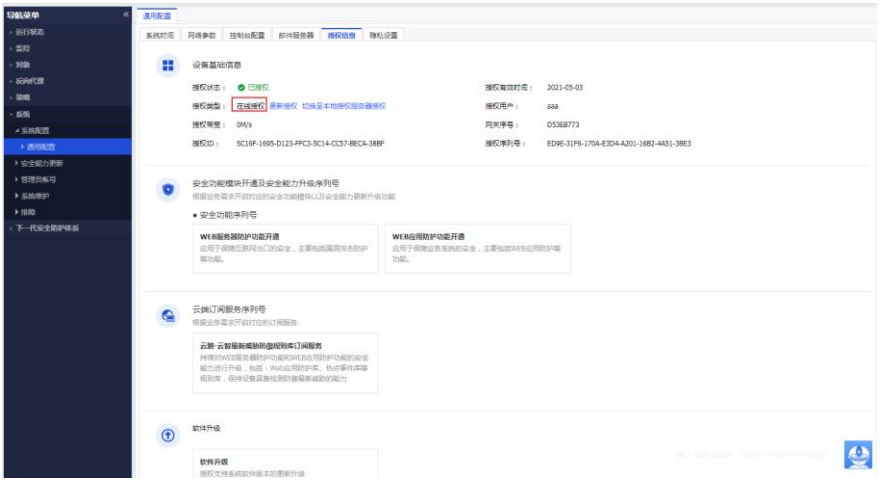
软件升级和维保服务：展示云WAF目前软件升级的有效限期，在限期内，可对云WAF进行版本的升级，保持云WAF在功能上的全面性。

通过联网时自动更新授权或设备时，通过手动更新授权，即可启动相应功能以及授权更新规则。

在线授权

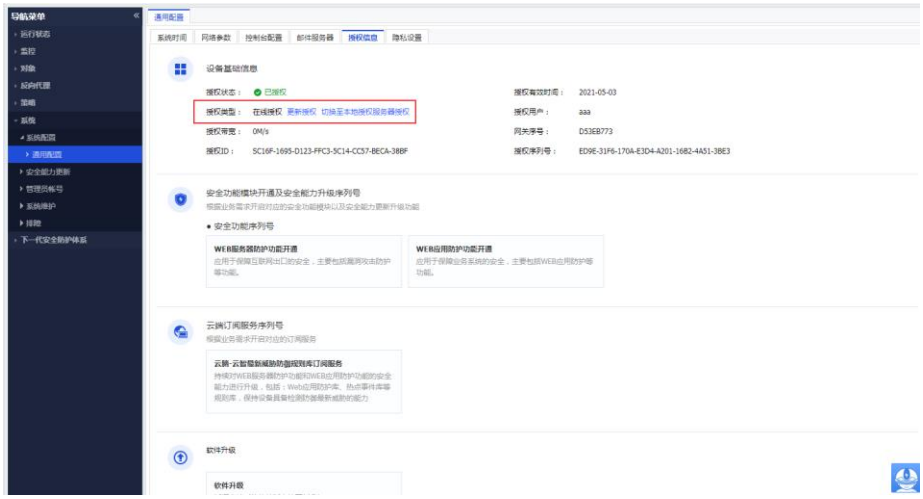
步骤1.在[系统/系统配置/通用配置/授权信息] 中配置云WAF3.0授权序列号，购买后提供信息联系深信服开通云端授权。

步骤2.点击使用在线授权，填写正式的序列号和ID。或者点击申请免费试用，填写试用序列号和ID。在线授权成功如图所示。



步骤3.切换在线授权的方式如下：

步骤4.点击切换在线授权，输入申请的序列号ID和序列号，点击确定即可。需要重新登录，登录后的在线授权状态如下图。

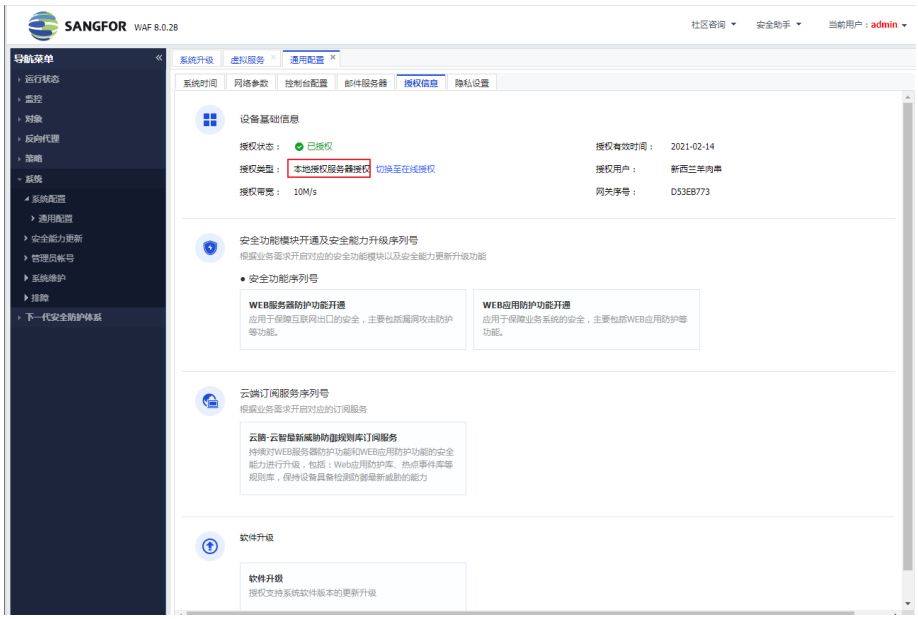


步骤5.在线授权有试用和正式2种序列号，如果一台设备没有授权过，可以申请试用序列号，试用时间为1个月。已经授权过的设备不能再申请试用序列号。

一个授权ID和序列号只能同时给一台设备使用。

离线授权

通过安装VLS的形式导入授权，从而提供给云WAF的授权。该方法需要VLS能够连接互联网，设备没有要求。



步骤1.在本地vls授权服务器给该设备配置授权，在设备的[系统/系统配置/通用配置/授权信息]里可以查看到本地授权服务器授权。

步骤2.如果没有授权状态如下图（既没有本地授权也没有在线授权），在本地vls授权服务器给该设备配置授权后，就如上图。

步骤3.也可以由在线授权状态切换成本地授权状态。点击切换至本地授权服务器授权，同时在本地授权服务器上授权该设备，然后等待几分钟后刷新页面即可切换成本地授权。

8.1.6. 隐私设置

隐私设置主要用于是否允许上报产品的用户体验改进内容。以进行产品的持续改进，给用户带来体验的提升。

参与用户体验改进计划：勾选后允许产品上报相应的体验改进内容。

授权云端安全防护：选择“授权云智更新安全能力库”后，只通过云端更新设备功能模块规则，不对未知威胁进行云端联动检测。

点击<确定>，完成功能生效。

8.2. 安全能力更新

安全能力升级用于在授权有效期内对设备内置库（漏洞攻击特征识别库、Web应用防护库、热点事件库）进行升级管理。以下表格是具体规则库说明。

表8 规则库说明表

库名称	说明
漏洞攻击特征识别库	所有系统漏洞、应用漏洞等攻击特征的集合，提供给漏洞攻击防护模板使用。
Web 应用防护库	所有 Web 应用攻击特征的集合，提供给 Web 应用防护模板调用。
热点事件库	近段时间的热点事件的集合，提醒客户及时发现存在的风险。

首先勾选序号前面的框，通过点击<启用>可开启内置库的自动升级，点击<禁用>可关闭内置库的自动升级，点击<刷新>用于看到内置库版本的实时信息。

规则库升级

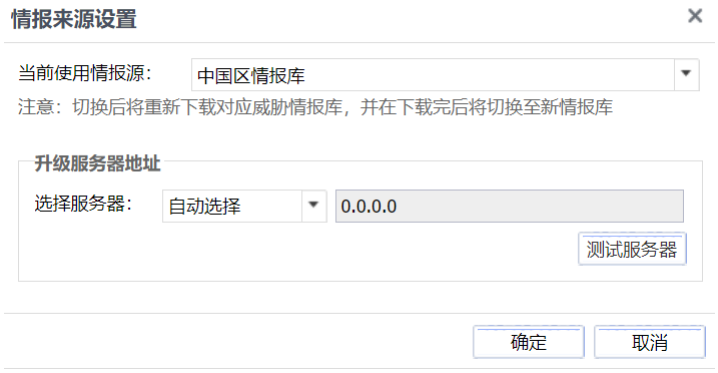
在设备不能联网的情况下，通过点击<离线升级>可以配置在升级服务有效期内的规则库的手动升级。

在设备已经联网的情况下，点击<立即更新>可　以对已选的有效期内的规则库立即进行在线更新。

情报来源设置

主要用于配置设备使用情报来源以及需要连接的升级服务器，情报来源切换后会重新下载对应的威胁情报库。

点击<情报来源设置>，进入[情报来源设置]页面，情报来源主要有中国区情报库和海外情报库，升级服务器可以实际的外网的线路进行选择，或选择自动选择让设备自动检测可以连接的更新服务器。



代理设置

当网络中有HTTP代理服务器时，配置好代理服务器，让设备可以通过代理服务器上网更新内置库，代理设置内置库升级需要设备本身是联网的状态。

点击<代理设置>，进入代理设置页面。勾选[启用代理服务器]，填写代理服务器的IP地址、端口，勾选<验证用户>输入代理服务器需要验证的用户名和密码。界面如下。

离线升级配置案例

某企业客户WAF部署在内网，不能联通外网，为保证设备安全防护能力，现需要对有效期内规则库进行更新。

以更新Web应用防护识别库为例，其他有效期规则库也是一样的操作，具体步骤如下。

步骤1.通过如下链接进入深信服社区选择对应云WAF版本的Web应用防护识别库进行下载，需要注册深信服社区账号。

链接地址：https://bbs.sangfor.com.cn。路径：自助服务›Web应用防火墙WAF。

规则类别	更新时间	说明	大小	MD5	下载
漏洞特征识别库	2020-11-10	仅限AF6.8及以上版本使用	18.00MB	64A27D40F08BBBB7BF0FE8A41B22733E	
热点事件预警与处置库(中文)	2020-11-06	8.0.8及以上版本使用	51.02MB	7F073E76875FE9E322838F9E99381A2F	
热点事件预警与处置库(英文)	2020-11-06	8.0.8及以上版本使用	50.22MB	77C426A1441C43212A9613FA17AFC35A	
WEB应用防护库	2020-10-30	仅限AF6.8及以上版本使用	7.32MB	CA63CFF296286343F8C095A17EEC0B3F	
应用识别库（中文）	2020-10-27	仅限AF8.0.14及以上版本使用	1.98MB	D28BD287CDC4E37BCD665BCE29D8D8F3	
应用识别库（英文）	2020-10-27	仅限AF8.0.14及以上版本使用	1.98MB	B0019843BB0B282D8A8F1E915A88D69C	
URL库(中文)	2020-10-22	8.0.14及以上版本使用	45.58MB	E29B4D480B9E5BB2F69575157CDB7EA1	
URL库(英文)	2020-10-22	8.0.14及以上版本使用	46.00MB	CF964507D13D95658862E86E40538789	
实时漏洞分析识别库	2020-10-10	仅限AF6.8及以上版本使用	3.48MB	B79D86B6574D0D1AF093D00A5A32557E	
僵尸网络与病毒防护库（国内库）	2020-09-02	仅限AF8.0.14及以上版本使用	98.17MB	1A64EEB34DAA4D819EDC3B9686F609A2	
僵尸网络与病毒防护库（海外库）	2020-09-02	仅限AF8.0.14及以上版本使用	97.25MB	9DC31B3FDB7E376413CD9444322CE78B	
热点事件库	2020-08-03	仅支持AF8.0.5及以上版本	1.50MB	60EFC4744DC26C5E4F13C00340FF8700	

步骤2.在[安全能力更新]页面选择Web应用防护识别库后，点击离线升级。如下图所示。

步骤3.进入[手动升级库]页面，点击<手动更新>，选择下载好的Web应用防护识别库。如下图所示。

步骤4.点击<确定>，等待更新完成后，可以查看到漏洞攻击识别库已更新成功。如下图所示。

8.3. 管理员账号

管理员账号用来设置能够通过控制台来管理设备的登录用户和管理员角色管理。设备出厂默认的管理员的账号密码为：admin/admin。在导航菜单页面中的[系统/管理员账户]，进入管理员账户编辑页面，进行新增、编辑、删除、启用和禁用操作。

[管理员账号]用来设置能够通过控制台管理设备的登录用户。[管理员账号]编辑页面如图所示。

默认有三个管理员角色，分别是安全管理员、审计员和系统管理员。

- 系统管理员：负责对软件环境日常运行的管理和维护，具有基础网络配置，用户管理等其他非安全策略的管理权限。
- 安全管理员：具有查看和修改安全策略的权限，日志查看权限。
- 审计员：只具有查看和修改内置数据中心的权限。
- 远程认证用户：可以在外部服务器选择用户作为管理员账号。

点击<新增>弹出[新增管理员账号]页面。如下图所示。

用户名：设置管理员账户名称。

描述：设置对该账户的描述。

新密码：设置管理员账户的密码。

确认新密码：重新输入新密码。

页面权限设置：用于设置对控制台和数据中心各个模块是否有可查看或可编辑权限。

点击<密码安全策略>，用于设置控制台管理员密码的安全策略，可设置下次登录是必须修改密码和密码最长使用天数。注意：只有admin管理员可以设置此功能权限。

点击<外部认证服务器>，用于有外部服务器进行管理员账号的认证，认证方式有TACACS和RADIUS服务器。如下图所示。

8.4. 排障

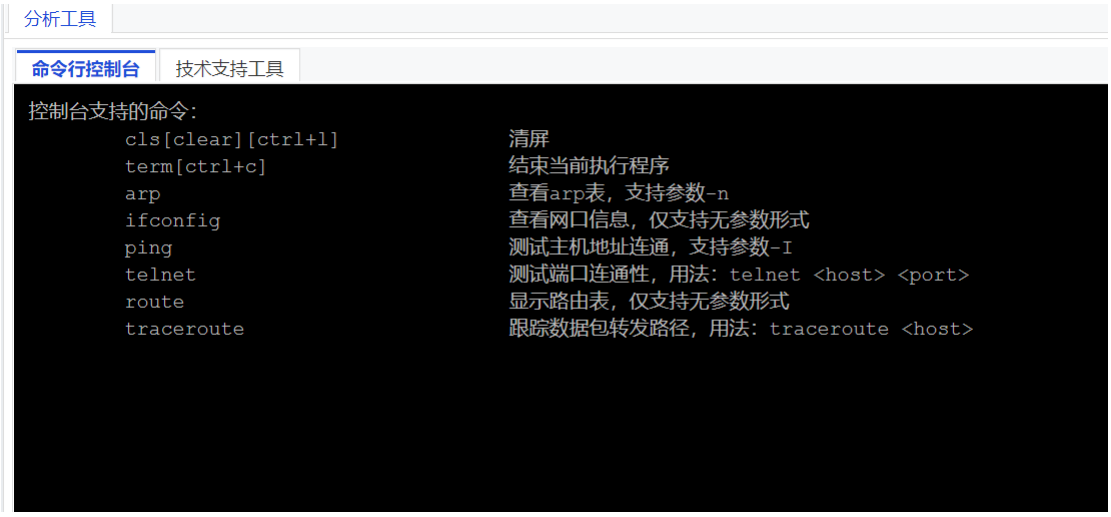
排障功能用于排查定位网络问题，方便管理员进行管理运维。

8.4.1. 分析工具

分析工具主要介绍命令行工具和技术支持工具使用。

8.4.1.1. 命令行工具

[命令行工具]提供一个简单的控制台命令行，可用于对设备的一些简单信息进行查看，支持的命令包括：cls（清屏）、term（结束当前执行程序）、、arp（查看arp表）、、ifconfig（查看网口信息）、、ping（测试主机地址连通）、telnet（测试端口连通性）、、route（显示路由表）和traceroute（跟踪数据包转发路径），在命令行页面直接输入命令回车即可，如下图所示。



8.4.1.2. 技术支持工具

[技术支持工具]用于技术支持人员对设备进行问题排查、巡检，方便对设备进行维护。

获取黑盒信息该功能主要是获取黑盒信息，可以下载黑盒信息，方便技术支持人员排查问题。

重置数据库：该功能主要用来重置数据库，重置数据库将清空内置数据中心的所有数据，请谨慎操作。

⚠ 注意：

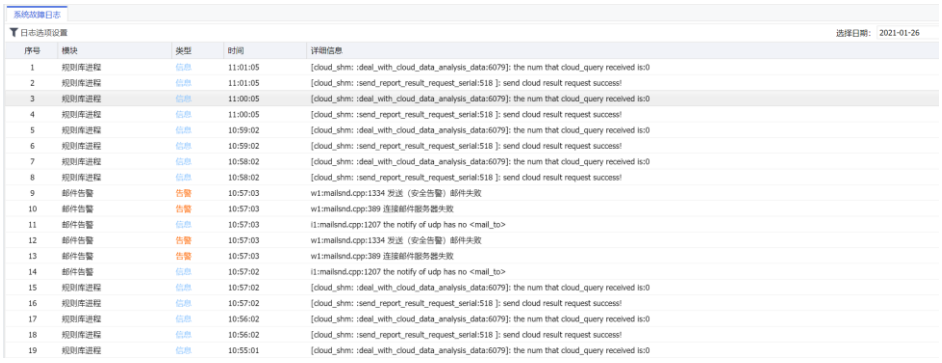
1、 重置数据将不能恢复；

2、 在查看安全日志或者系统日志，提示报错时，可以使用该功能。

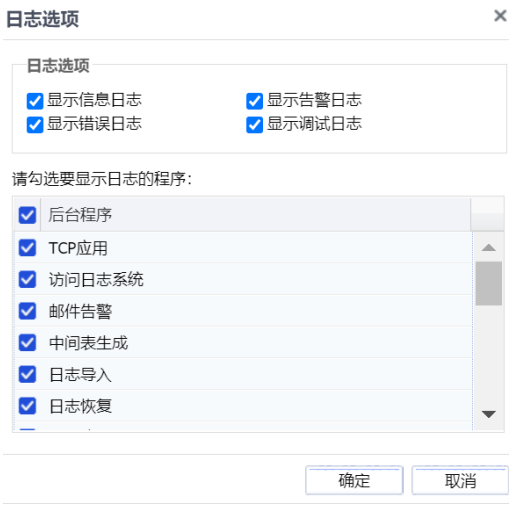
设备巡检：该功能支持一键对WAF进行产品状态巡检，并生成巡检报告。巡检内容包括：设备巡检概况、设备负载、网络连通性、业务状态、日志合规性、系统运行状态、进程检查、配置状况、版本历史重大BUG、Dmesg检查共10项检查。

8.4.2. 系统故障日志

[系统故障日志]用于查看设备各模块运行状态日志，可通过日志判断设备各模块是否正常运行，如下图所示。



点击<日志选项设置>，出现[日志选项]页面，选择要查看的日志类型，如下图所示。



点击<提交>后，即显示所选日志信息。

8.5. 系统维护

系统维护是指为适应系统的环境和其他因素的各种变化、保证系统正常工作而对系统所进行的修改，包括备份与恢复、系统升级、重启网关等功能模块。

8.5.1. 备份与恢复

[备份与恢复]用于将设备的配置下载到本地保存，或者是将原有的备份的配置文件恢复到设备中。

备份配置：用于备份下载设备中已有的配置，点击<下载当前配置>，就可以对当前的配置进行备份。

恢复配置：用于恢复已备份的配置文件。恢复配置文件有两种方式：

方式一：从自动备份中恢复，设备会在每日凌晨自动备份一次配置，默认保存一周的配置文件，选择要恢复的配置文件，点击<恢复>即可。

方式二：从本地文件中恢复，点击<浏览>，并打开备份文件，点击<恢复>即可恢复备份配置。

恢复出厂配置：从默认配置中恢复，点击<恢复出厂配置>，可以将设备恢复到出厂状态。

⚠ 注意：

恢复配置或者恢复出厂配置都会导致设备重启，请在恢复之前确认是否可以断网，建议在无业务或者业务低峰时间段操作，避免影响正常业务。

8.5.2. 系统升级

系统升级支持从设备界面加载升级包升级系统版本。新版本发布后，判断升级条件满足，需要版本更新时，点击<离线升级 >，显示<上传本地升级包>，加载本地升级包升级即可。

详细步骤在产品升级指导，有两种操作升级方式，控制页面升级和客户端升级。

点击[查看升级历史]，可以查看历史的升级记录。

8.5.3. 重启网关/服务

重启设备：设备直接重启，会造成业务全部中断大于5分钟。

重启所有服务：重启设备的服务，会造成业务闪断，谨慎操作。

9. 下一代安全体系

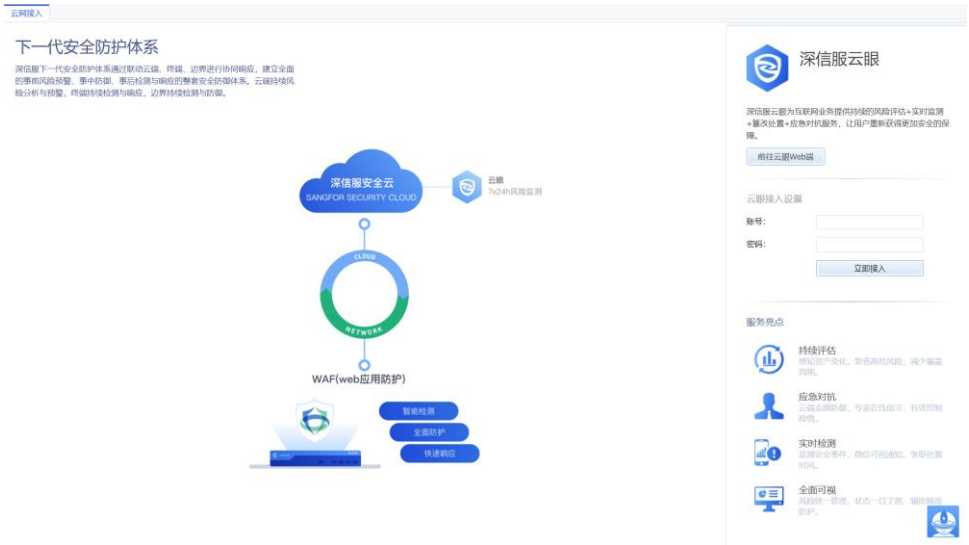
下一代安全防护体系通过联动云端进行协同响应，建立全面的事前风险预警、事中防御、事后检测与响应的整套安全防御体系。

9.1.1. 云网联动

云网联动用于设置设备与云端的接入与联动操作。

9.1.1.1. 云网接入设置

[云网接入设置]设置目前AF可以联动响应的云端产品。如下图所示。



云眼

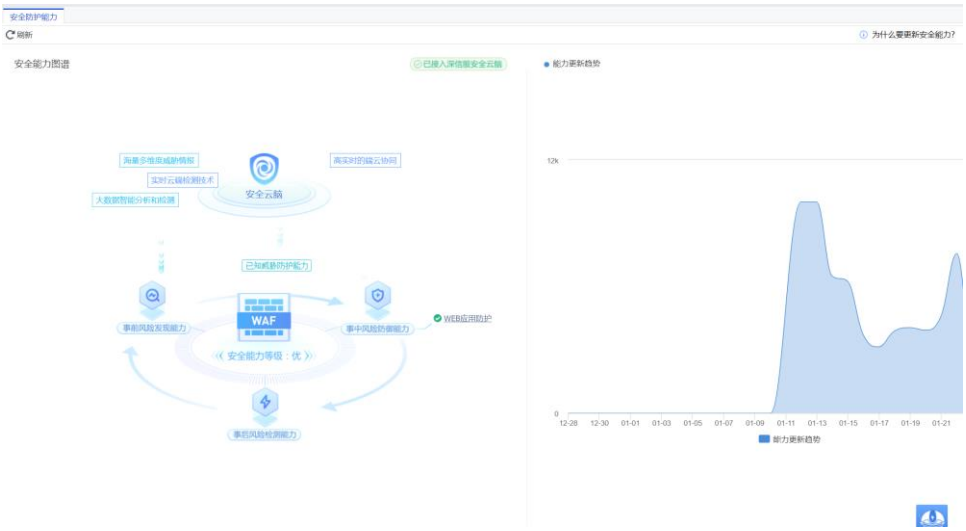
深信服云眼为互联网业务提供持续的风险评估+实时监测+篡改处置+应急对抗服务，让用户重新获得更加安全的保障。

设备可以访问互联网，同时已开通云眼，并在云眼平台完成了相关监测网站的绑定。此处可通过所开通的云眼账号，完成与云眼平台的对接。输入开通的云眼账号和密码，如下图所示。

点击<立即接入>，接入成功后，就能在云眼平台上对绑定的监测网站进行监测。

9.1.2. 安全防护能力

安全防护能力用于展示设备的更新能力，包括安全能力图谱、能力更新指标部分内容。如下图所示。

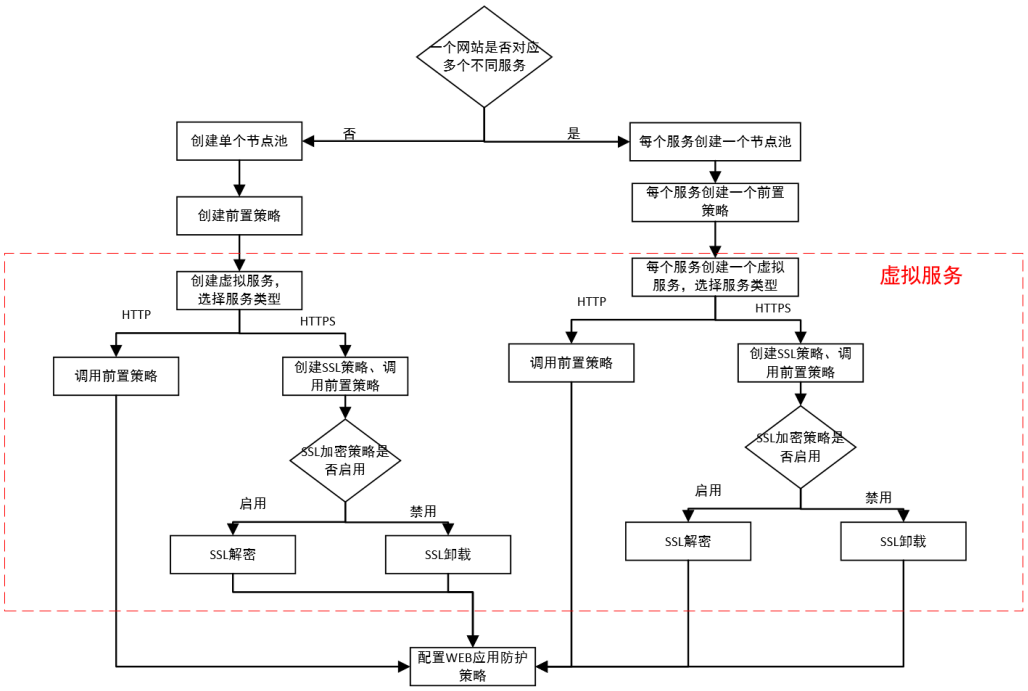


安全能力图谱：以图例方式展示AF与其它深信服产品的联动更新过程，完成“事前风险发现能力”、“事中风险防御能力”和“事后风险检测能力”的实时更新。

能力更新指标：以趋势图的方式展示持续更新的能力和相关热点事件的实时数据。

10. 典型场景案例集

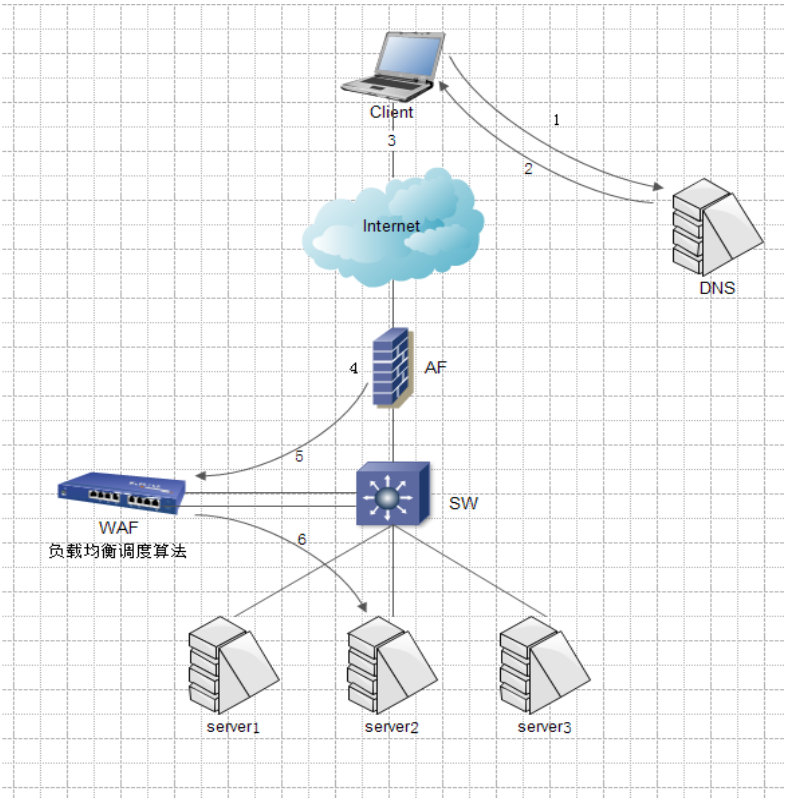
典型场景案例集主要介绍WAF在典型网络环境下的配置案例。整体的配置思路如下图所示。



10.1. 反向代理案例配置_HTTP

10.1.1. 需求背景

客户业务中存在3台HTTP服务器，在业务高峰期时，某台服务器经常存在负载过高的情况。同时，经常遭受来自互联网的扫描攻击，给服务器带来较大风险。因此，需要对外隐藏真实的服务器，减少攻击带来的风险。对内需要将业务负载到各个服务器上，从而减少负载过高的情况。

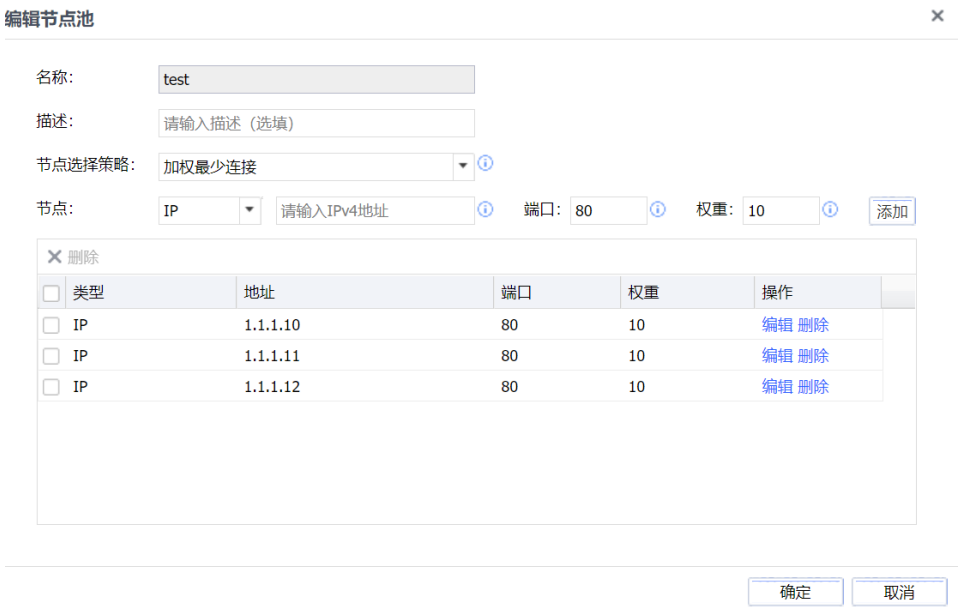


10.1.2. 需求分析

Web服务器遭遇到互联网攻击，需要使用WAF来防护Web服务器的安全。同时，需要隐藏物理服务器的IP，可以通过反向代理来进行设置。反向代理可以通过算法来把业务负载到各个物理服务器上，从而减少某台服务器负载过高的问题。

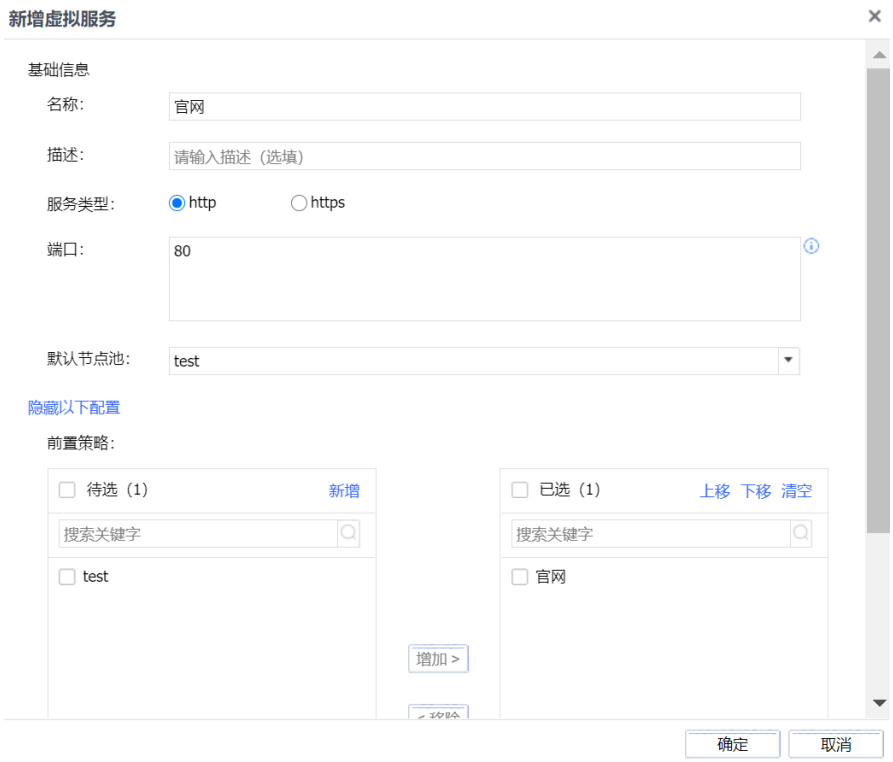
10.1.3. 配置步骤

步骤1.创建节点池，对节点使用不同的负载均衡算法进行调度到各个服务器上，如下图所示。

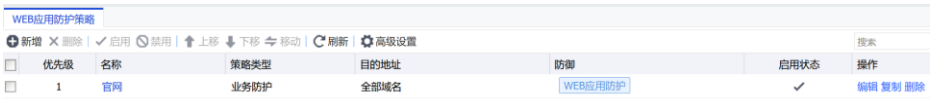


步骤2.创建前置策略，将不同的访问源调度到指定节点上，如下图所示。

步骤3.创建虚拟策略，将服务对外发布，如下图所示。



步骤4.配置安全策略，对指定的应用进行安全检测，如下图所示。

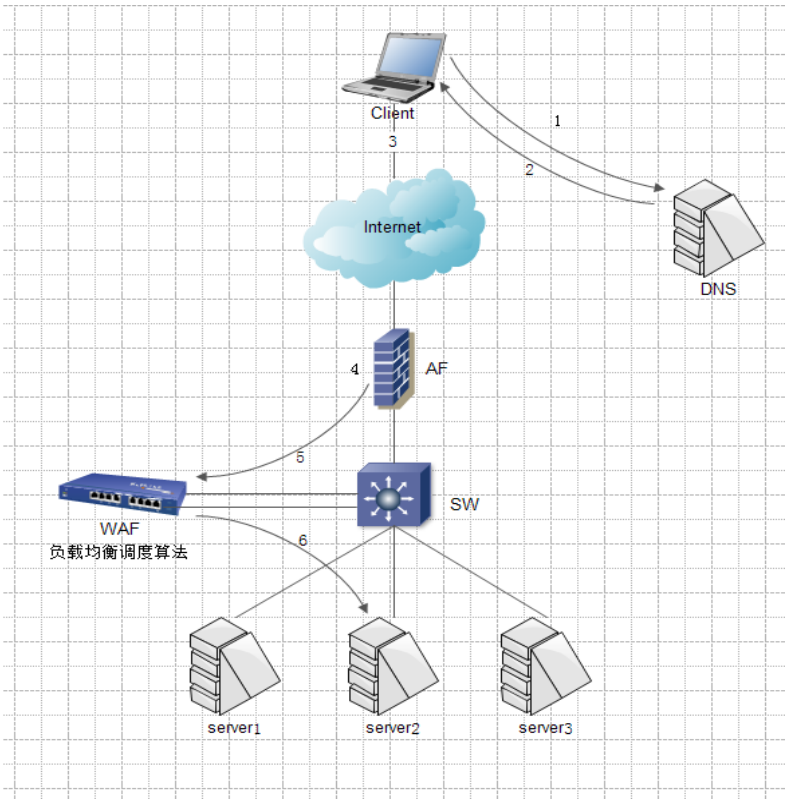


步骤5.访问WAF的IP和端口，返回服务器的内容，如下图所示。

10.2. 反向代理案例配置_HTTPS 解密

10.2.1. 需求背景

某企业使用云WAF做Web服务器的防护，但是该Web服务器运行的站点是HTTPS。用户要求对Web的攻击行为进行安全检测和拦截，并能够发现那些IP对站点发起攻击行为。

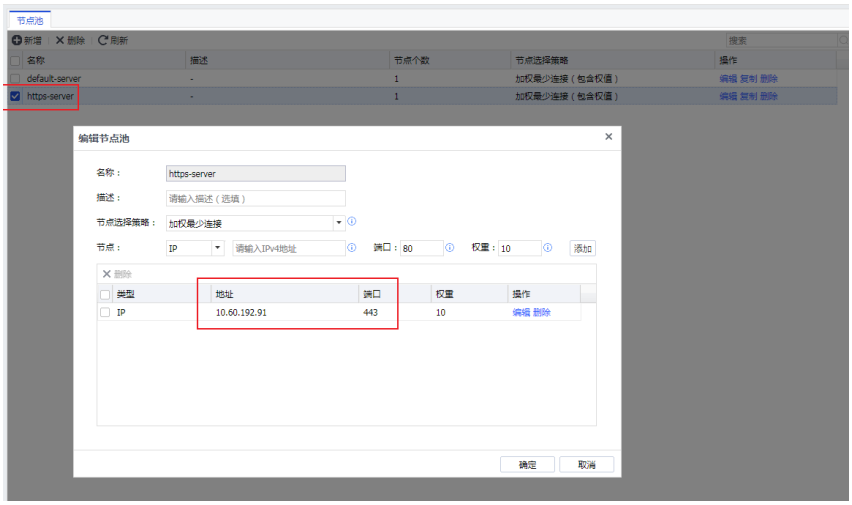


10.2.2. 需求分析

针对这些需求，需要使用HTTPS解密功能，来对HTTPS流量进行解密，然后发现存在的攻击行为。

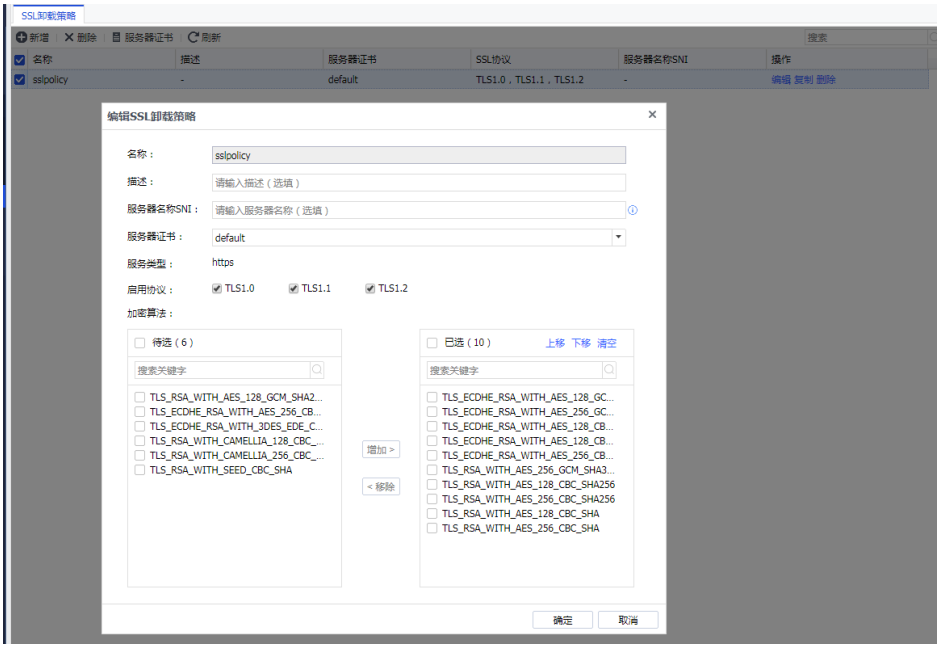
10.2.3. 配置步骤

步骤6.创建节点池https-server配置https服务器，提供给前置策略使用，如下图所示。

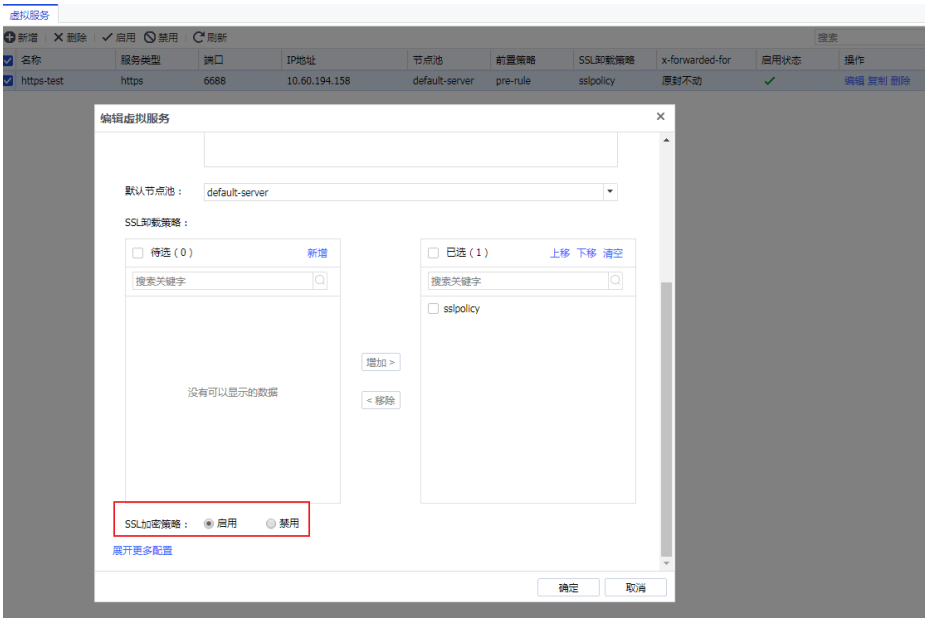


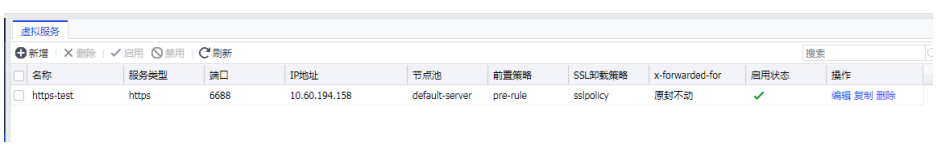
步骤7.配置前置策略pre-rule，调度节点池配置https-server节点池，如下图所示。

步骤8.配置ssl策略，如下图所示。

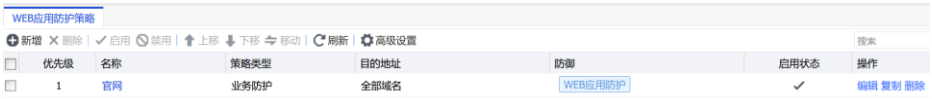


步骤9.配置虚拟服务https-test，如下图所示。



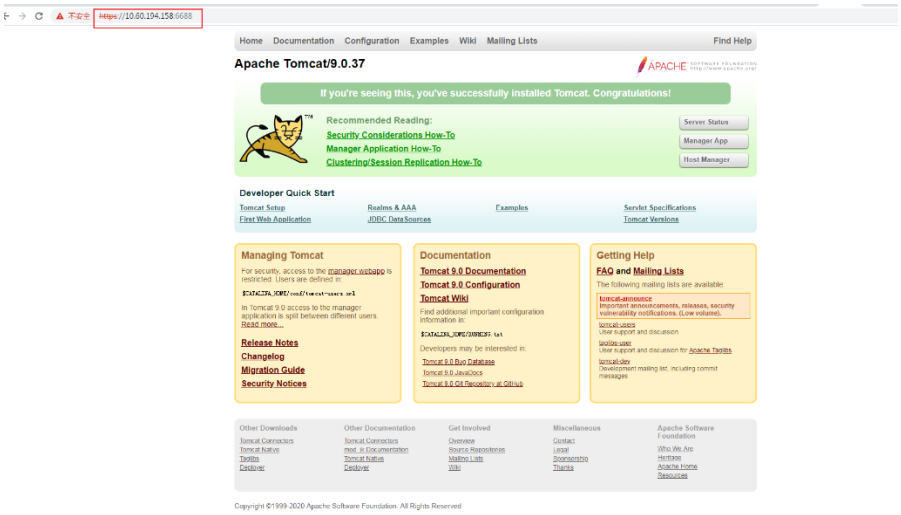


步骤10.配置安全策略，对指定的应用进行安全检测，如下图所示。



10.2.4. 效果预览

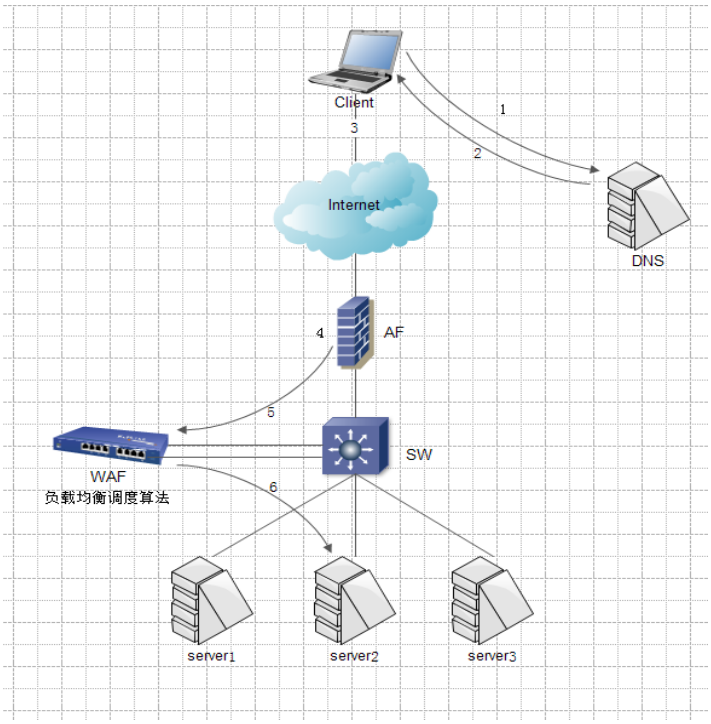
1. 使用浏览器访问虚拟服务https://10.60.194.158:6688/，成功访问到前置策略配置的https服务器节点。



10.3. 反向代理案例配置_HTTPS 卸载

10.3.1. 需求背景

某企业使用云WAF做Web服务器的防护，但是该Web服务器运行的站点是HTTP。为了防止数据在公网中给截取和篡改，需要在不改变HTTP服务器的情况下，要求客户端与WAF之间使用HTTPS的形式交互，WAF与服务器之间使用HTTP的形式交互。同时，用户要求对Web的攻击行为进行安全检测和拦截，并能够发现那些IP对站点发起攻击行为。

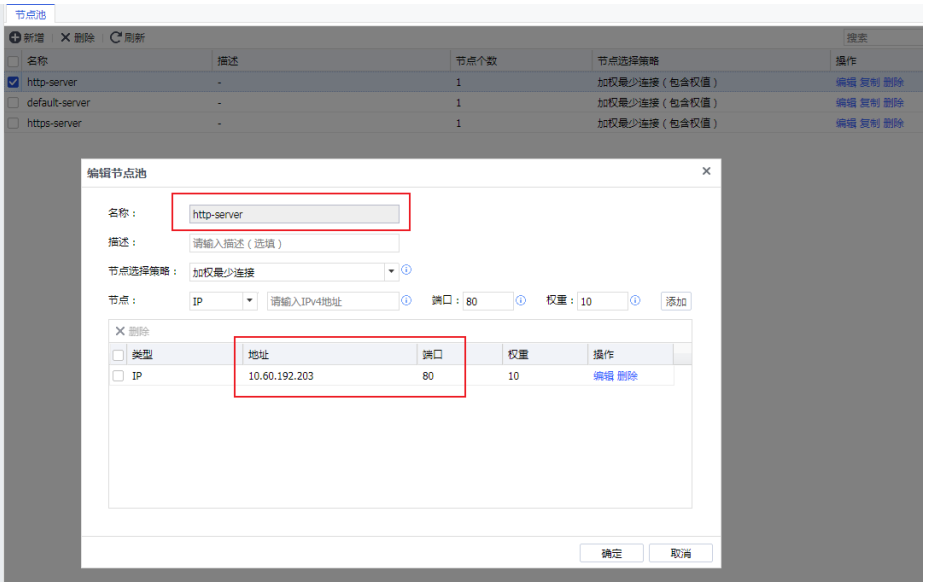


10.3.2. 需求分析

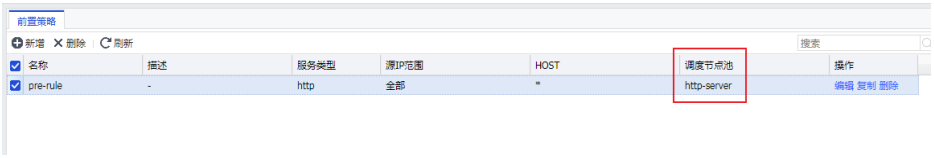
针对这些需求，需要使用HTTPS卸载功能，在客户端与WAF之间交互中通过加密的形式，把流量加密成HTTPS。WAF与Web服务器之间对HTTPS流量进行卸载，以HTTP的形式交互。

10.3.3. 配置步骤

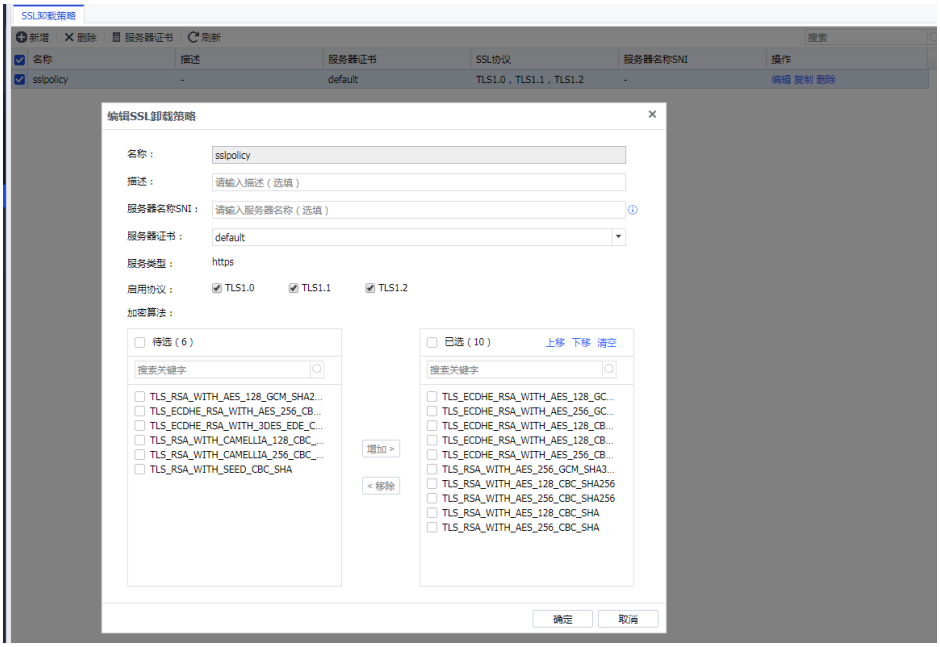
步骤1.创建节点池http-server配置http服务器，提供给前置策略使用，如下图所示。



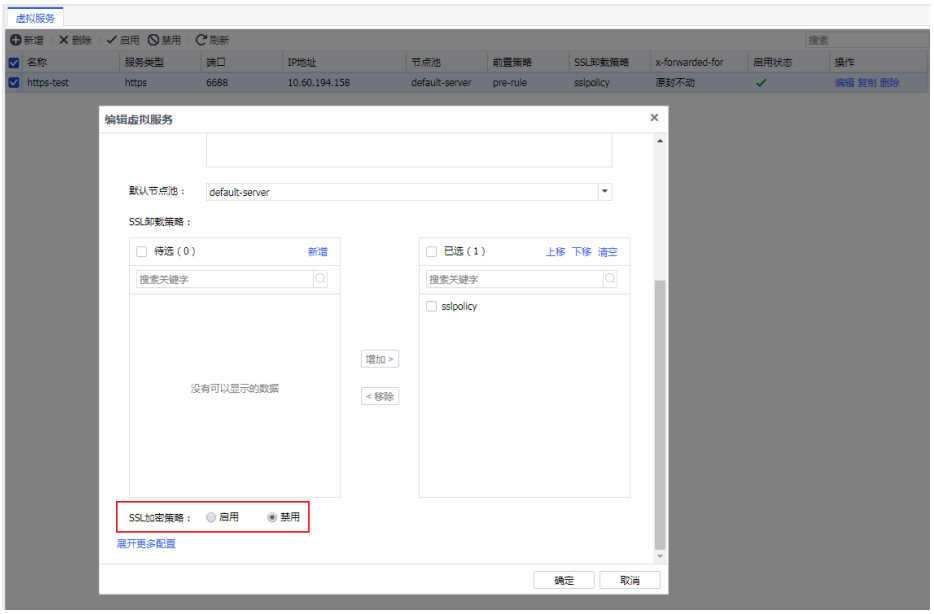
步骤2.配置前置策略pre-rule，调度节点池配置https-server节点池，如下图所示。

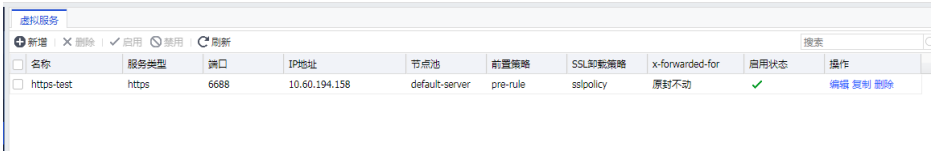


步骤3.配置ssl策略，如下图所示。

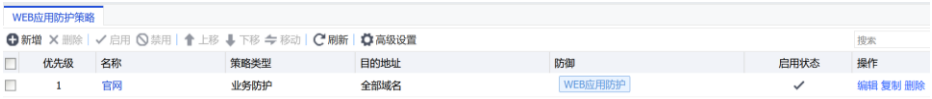


步骤4.配置虚拟服务https-test，如下图所示。





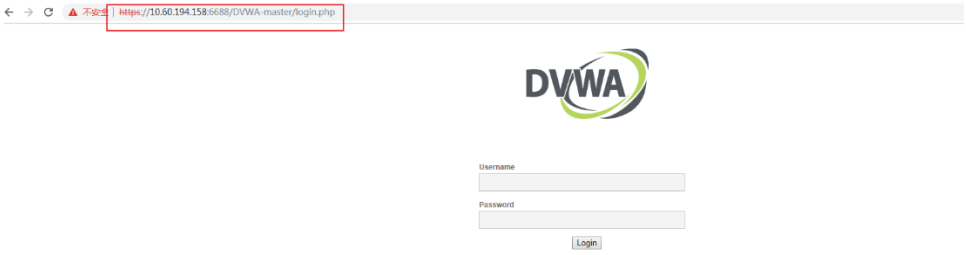
步骤5.配置安全策略，对指定的应用进行安全检测，如下图所示：



10. 3. 4. 效果预览

使用浏览器访问虚拟服务

https://10.60.194.158:6688/DVWA-master/login.php，成功访问到前置策略配置的http服务器节点。



11. 运维管理

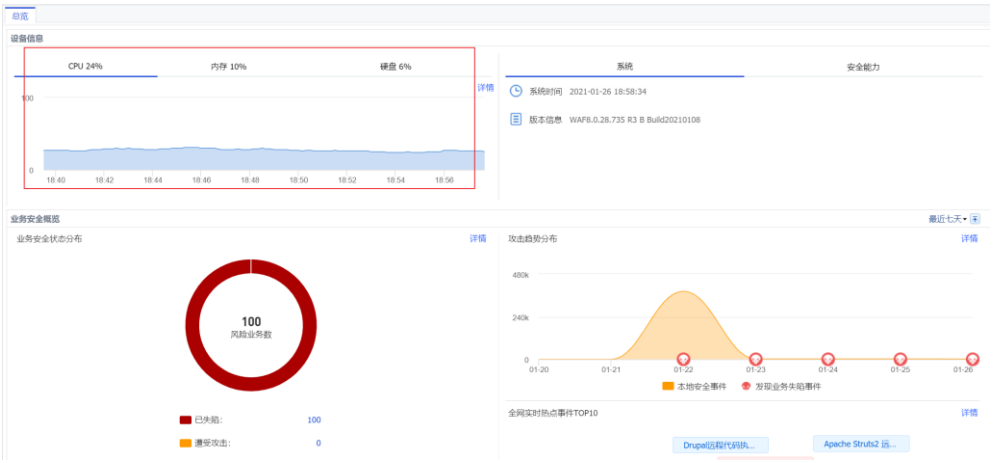
本章主要讲解产品的运维管理，为管理员例行维护设备以及简单故障排除提供指导。

11.1. 日常巡检

日常巡检主要是为了保证设备正常运行，防止设备出现异常影响到业务的运行，从而带来较大的风险。

11.1.1. 设备运行检查

通过设备控制台的设备状态，检查CPU、内存、磁盘占用率是否长期居高，如果CPU、内存长期居高，请按照如下步骤进行操作。登录设备后显示的总览就是设备状态。



11.1.2. 设备配置信息检查

11.1.2.1. 设备配置备份

为了保证网络的稳定运行，建议客户每个月进行一次配置的备份，以防止云WAF系统意外瘫痪导致系统无法迅速恢复。

方法：登陆云WAF控制台，点击[系统/系统维护/备份与恢复]，点击<下载当前配置>下载配置并妥善保存即可，如下图所示。

11.1.2.2. 规则库版本检查

为了确保设备能够正常识别最新的网络应用，建议定期检查设备规则库是否更新，如果更新异常，请检查设备自身能否访问外网。

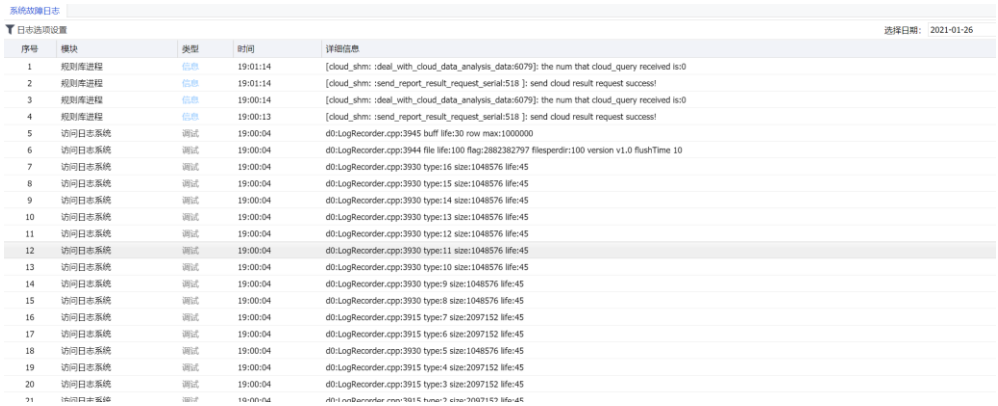
11.1.3. 设备安全检查

11.1.3.1. 控制台账号安全性检查

1. 控制台管理员密码是否为默认的admin或123456之类的简单密码。如果是默认密码或简单密码，请立即修改密码。
2. 控制台管理员密码一个月内有没有修改过，如果控制台管理员密码一个月内都没有修改过，请立即修改并妥善保存密码。
3. 控制台是否有多余账号，如sangfor、test以及公司英文等不必要的简单账号，如果有的话，请删除多余账号，仅保留授权的管理员账号。

11.1.3.2. 设备日志信息检查

通过[系统/排障/系统故障日志]，可以看到设备各模块运行状态日志，可通过日志判断设备各模块是否正常运行。



系统日志包含信息、告警、错误、调试四个级别，点击<日志选项设置>，可以过滤需要查看的级别以及模块的日志。

如果系统日志中出现大量错误日志和告警日志，请及时联系深信服技术支持工程师，确认是否设备程序运行故障。

11.2. 辅助工具使用

11.2.1. 命令控制台

SANGFOR WAF命令控制台提供一个简单的控制台命令行界面，可用于对设备的一些简单信息进行查看，支持的命令包括：

vlan(查看vlan上的接口)

arp（查看设备的arp表）

ifconfig（查看设备网口信息）

ping（测试主机地址的连通性）

telnet（测试端口连通性）

route（显示设备的路由表）

traceroute（跟踪数据包转发路径）

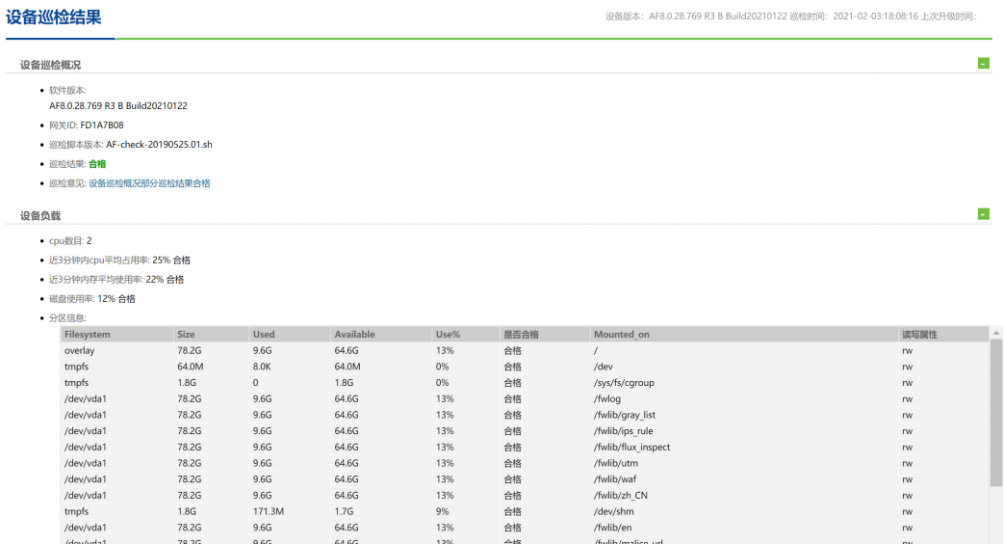
在[系统/排障/分析工具]页面直接输入命令回车即可，ping、telnet、traceroute命令用法和PC相同。

11.2.2. 设备巡检

为了保证设备的稳定运行，建议客户每个月对设备进行一次巡检，设备软件版本在8.0.28及以上的直接在控制台页面上进行巡检。

方法：登陆WAF控制台，点击[系统/排障/分析工具]，选择技术支持工具，在设备巡检选项中点击<开始巡检>即可进行巡检并弹出设备巡检结果页面。

具体巡检结果如下，如有不合格的选项，可参考巡检意见进行调整。如下图所示。



12. 产品升级指导

产品升级指导主要介绍设备系统升级的具体方法以及升级前后的检查。

12.1. 产品升级步骤

1. 内网升级场景，升级前需提前准备好升级包，确保升级包的完整性。
2. 在[深信服社区/自助服务/软件下载/Web应用防火墙]获取升级包下载链接，下载并保存到电脑本地。
3. 使用MD5校验工具校验升级包的MD5，保障升级包的完整性。
4. 在线升级场景，升级前需保障待升级设备和服务端网络畅通。

12.2. 产品升级前检查

升级前需要确认本版本是否支持直接升级到目标版本，升级是否影响老功能特性，升级后是否需要重启，升级时间估算，用户配置、日志、数据是否平滑升级、升级限定条件。请先登录深信服社区，访问如下链接查找目标版本升级文档确认升级细节：https://bbs.sangfor.com.cn/plugin.php?id=service:download&action=view&fid=100000003677756#/100000011367652/all/undefined

12.3. Web 系统升级指导

Web系统升级方法用于升级要求方法简明，设备本身可以访问公网或者云端服务器已放置升级包等升级场景使用，这种升级方式升级过程更加直观，升级过程更透明，无需额外工具配合。

12.3.1. Web 系统升级步骤

Web系统升级只支持离线升级。

进入设备Web控制台[系统管理/系统更新/系统升级]路径后，点击<升级到其他版本>按钮，上传本地升级包，并按照提示操作，完成升级。

12.3.2. Web 系统升级操作方法

步骤1.进入[系统/系统维护/系统升级]页面，如下图所示。

步骤2.点击<离线升级>，进入到[准备升级包]页面，如下图所示。

步骤3.点击<上传本地升级包>，选择下载好的版本升级包进行上传，如下图所示。

注意：

上传升级包过程中不能关闭该页面，否则需要重新进入页面再执行升级操作。

步骤4.升级包上传完成后，点击<下一步>完成配置的备份即可开始升级，升级完成后设备自动重启。完成重启后，登录设备控制台，检查设备升级后状态。

12.4. 产品升级后检查

设备健康检查：

序号	检查项	检查要求
1	设备 CPU 使用率是否正常	正常情况，CPU 平均使用率应 70%以下。
2	设备内存使用率是否正常	正常情况，内存平均使用率应 70%以下。
3	系统日志是否有错误或告警日志	正常情况系统日志应无错误日志，异常情况请联系厂商处理。
4	检查是否有备份设备配置	实施完成后，应该备份设备配置，本地存档。
5	规则库是否升级到最新	基于应用识别准确度考虑，要求实施完成后，保证当前规则库更新到最新。