



深信服云 WEB 应用防火墙

快速安装手册

产品版本 8.0.61

文档版本 02

发布日期 2022-08-16

深信服科技股份有限公司

版权声明

版权所有 © 深信服科技股份有限公司 2022。保留一切权利（包括但不限于修订、最终解释权）。

除非深信服科技股份有限公司（以下简称“深信服公司”）另行声明或授权，否则本文件及本文件的相关内容所包含或涉及的文字、图像、图片、照片、音频、视频、图表、色彩、版面设计等的所有知识产权（包括但不限于版权、商标权、专利权、商业秘密等）及相关权利，均归深信服公司或其关联公司所有。未经深信服公司书面许可，任何人不得擅自对本文件及其内容进行使用（包括但不限于复制、转载、摘编、修改、或以其他方式展示、传播等）。

特别提示

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，如有变更，恕不另行通知。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，深信服科技股份有限公司不对本文档中的遗漏、变更及错误所导致的损失和损害承担任何责任。

联系我们

售前咨询热线：400-806-6868

售后服务热线：400-630-6430（中国大陆）

深信服科技官方网站：www.sangfor.com.cn

7*24小时智能客服，排障咨询好帮手：

https://bbs.sangfor.com.cn/plugin.php?id=common_plug:online&ref=文档



打开微信扫一扫
可在手机端咨询

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。

日期	文档版本	修改内容
2022-08-16	01	文档第一次发布。

符号说明

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	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	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	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	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	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。

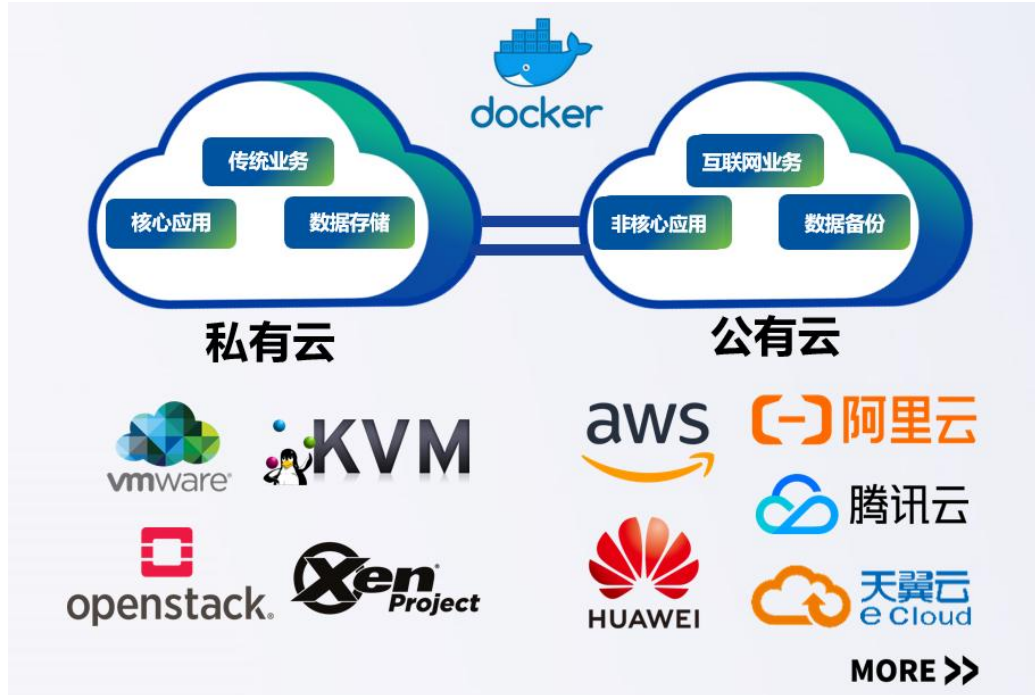
目录

目录.....	II
1. 产品介绍.....	4
1.1. 部署角色.....	4
1.2. 部署模式.....	5
1.2.1. 单台设备.....	6
1.2.2. 分离式设备.....	7
1.3. 集群部署.....	8
1.3.1. 反向代理模式.....	8
1.3.2. 插件模式.....	8
2. 部署准备条件.....	10
2.1. 环境要求.....	10
2.2. 硬件资源要求.....	10
2.3. 插件环境要求.....	11
3. 设备部署.....	12
3.1. 创建虚拟机.....	12
3.1.1. 私有云环境.....	12
3.1.2. 公有云环境.....	19
3.2. 安装 CENTOS 系统.....	46
3.3. 安装云 WAF.....	52
3.3.1. 单台设备反向代理模式.....	52
3.3.2. 单台设备插件模式.....	56
3.3.3. 分离式设备反向代理模式.....	60
3.3.4. 分离式设备插件模式.....	67
3.4. 登录云 WAF.....	75
3.5. 云 WAF 授权.....	76
3.6. 检查检测节点是否上线.....	78
3.7. 集群部署.....	79
3.7.1. 分离式设备反向代理模式集群.....	79
3.7.2. 分离式设备插件模式集群.....	82
4. 基本功能配置.....	84
4.1. 反向代理模式.....	84
4.1.1. HTTP 站点防护配置案例.....	84
4.1.2. HTTPS 站点防护配置案例_HTTPS 解密.....	91
4.1.3. HTTPS 站点防护配置案例_HTTPS 卸载.....	100
4.1.4. 一个 HTTP 端口负载多个 HTTP 站点防护配置案例.....	110

4.1.5. 站点策略 BOT 防护配置案例	119
4.2. 插件模式	127
4.2.1. HTTP/HTTPS 站点防护配置案例	127
5. 常见问题	134
5.1. 云 WAF 依赖包安装常见问题解决办法	134
5.2. 云 WAF 安装常见问题解决办法	134
6. 注意事项	136

1. 产品介绍

深信服云Web应用防护系统（简称云WAF）支持镜像和容器，创新融入容器技术的云WAF软件可灵活部署在VMware、KVM、Xen、OpenStack等各类虚拟化环境，并已经完美适配阿里云、腾讯云、华为云、电信云、AWS等公有云平台。



云WAF专注于网站、业务系统、API接口等安全防护，解决传统WAF安全产品易误报漏报、难以结合业务特点深度防御的问题，基于攻防情报、智能语义、主动验证Bot防护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。

1.1. 部署角色

云WAF支持管理节点和检测节点部署在同一台宿主机上，即云WAF单台设备部署，也支持管理节点与检测节点分离式部署，且一台管理节点可以对接多台检测节点。

序号	部署角色	说明
01	Management Platform + WAF Agent	同时部署管理节点和检测节点，适用于设备单台设备部署。
02	Management Platform	仅部署管理节点，适用于设备分离式部署。

03	WAF Agent	仅部署检测节点，适用于设备分离式部署。
----	-----------	---------------------

单台设备部署



管理节点和检测节点分离式部署



1.2. 部署模式

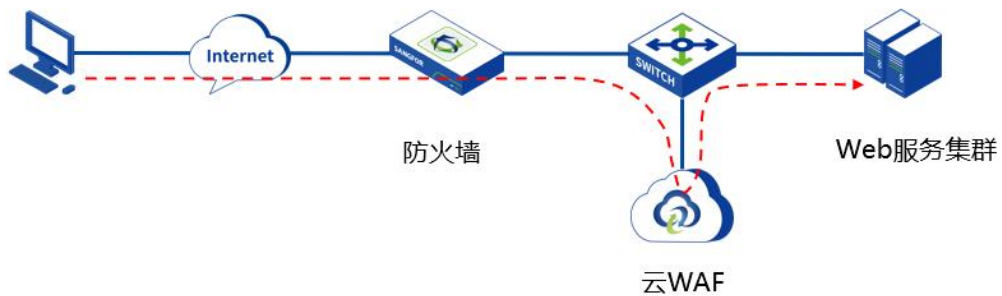
云WAF支持反向代理和插件两种模式。

序号	部署模式	说明
01	Reverse Proxy	反向代理模式，云 WAF 自带 nginx 反向代理服务
02	Plugin	插件模式，需要额外在客户自己的 nginx/tengine 服务器上安装插件，引流到云 WAF 的检测节点进行业务防护。

1.2.1. 单台设备

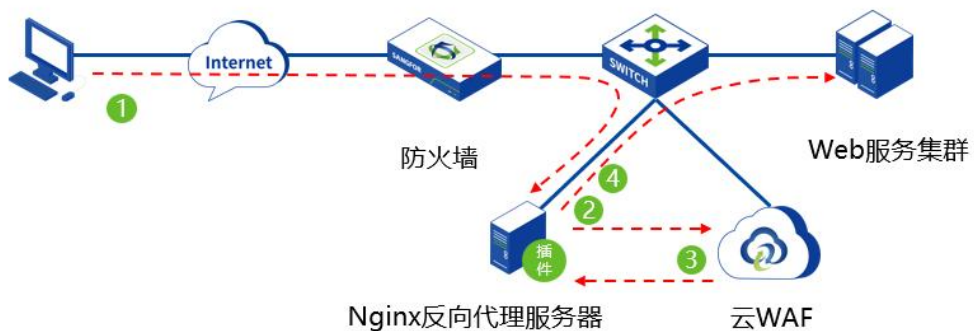
1.2.1.1. 反向代理模式

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，匹配对应的转发服务器，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。



1.2.1.2. 插件模式

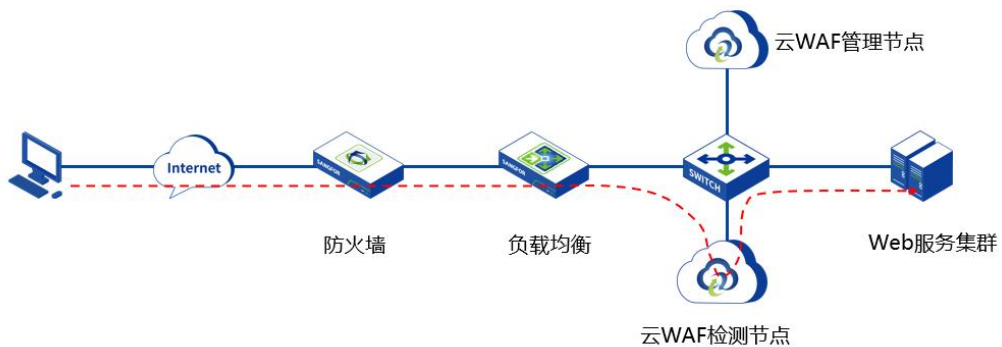
云WAF部署在客户虚拟环境或者云平台中，无需改变网络环境，在Nginx/tengine服务器上安装云WAF插件，由云WAF插件将Nginx的流量引流到云WAF的检测节点，经过云WAF检测节点的安全检测。经过云WAF的安全防护后，再由Nginx/tengine服务器将流量负载到各个节点业务服务器上。在整个过程中，由云WAF插件将流量引流到云WAF检测节点，检测节点对流量进行安全防护。



1.2.2. 分离式设备

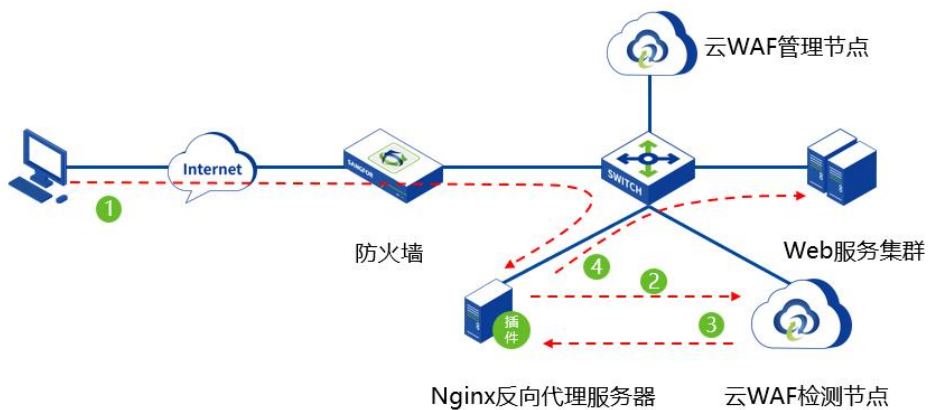
1.2.2.1. 反向代理模式

云WAF的管理节点和检测节点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检测节点后，匹配对应的转发服务器，将流量负载到各个节点业务服务器上。在整个过程中，云WAF检测节点起到反向代理作用，并对流量进行安全防护，并将日志上报到云WAF管理节点。



1.2.2.2. 插件模式

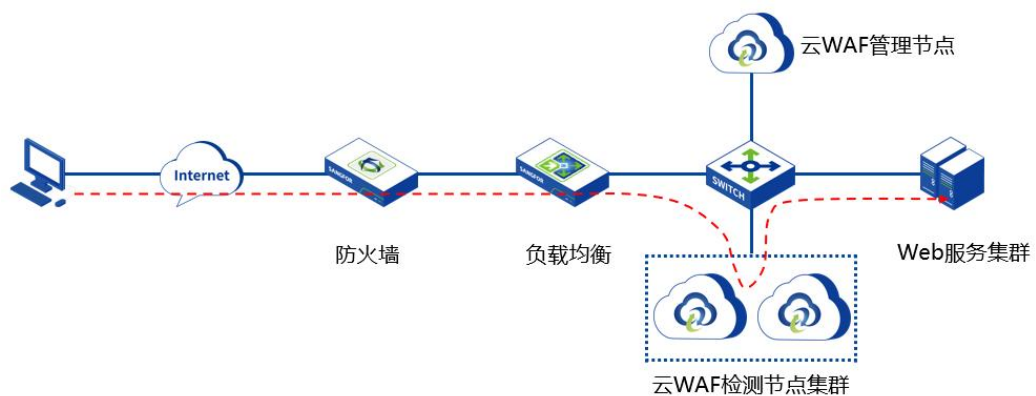
云WAF部署在客户虚拟环境或者云平台中，无需改变网络环境，在Nginx/tengine服务器上安装云WAF插件，由云WAF插件将Nginx的流量引流到云WAF的检测节点，经过云WAF检测节点的安全检测，再由Nginx/tengine服务器将流量负载到各个节点业务服务器上。在整个过程中，由云WAF插件将流量引流到云WAF检测节点，检测节点对流量进行安全防护，并上报日志到管理节点。



1.3. 集群部署

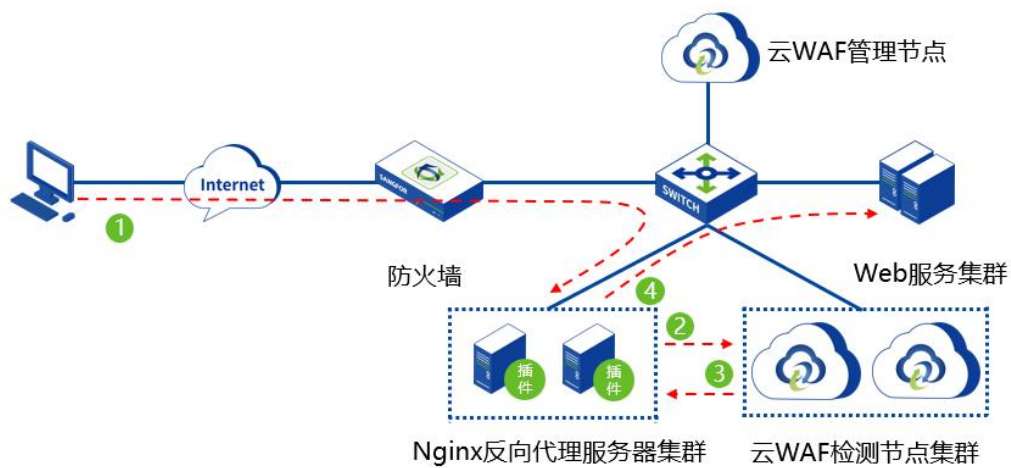
1.3.1. 反向代理模式

企业环境中，为了解决业务的可靠性和弹性伸缩需求，可以部署多台云WAF检测节点，对接同一台管理节点的方式实现。通过负载均衡设备把业务流量负载到各个云WAF的检测节点中，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检测节点，只需要在负载均衡设备中将云WAF添加到对应的组中即可。



1.3.2. 插件模式

企业环境中，为了解决业务的可靠性和弹性伸缩需求，可以部署多台云WAF检测节点，对接同一台管理节点的方式实现。通过Nginx服务器把业务流量负载到各个云WAF的检测节点中，流量经过云WAF的安全检测后，再由Nginx/tengine服务器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检测节点，只需要在Nginx/tengine服务器上的引流插件添加云WAF检测节点，并配置负载策略即可。



2. 部署准备条件

2.1. 环境要求

深信服云WEB应用防火墙的部署环境要求如下：

序号	环境	要求
01	宿主机环境	单台设备部署需要准备一台宿主机，分离式部署根据需求准备 2 台及以上宿主机。宿主机上仅支持单独部署 WAF 服务，不支持存在用户其他任何业务。
02	宿主机操作系统	操作系统仅支持 Cent OS，版本范围为 7.3-8.5，推荐 Cent OS 7.9，不推荐使用桌面版。
03	宿主机安装 docker	需提前安装 Docker-ce，并启动 docker，docker 版本最低支持 18.06.0，此项可通过云 WAF 依赖安装包解决。
04	宿主机安装 unzip	需提前安装 unzip，联网环境下可通过 yum -y install unzip 安装，离线环境下可以将 unzip 安装包上传到宿主机上，使用 rpm -Uvh [unzip 包名] 安装。安装完成后，可以使用 rpm -qa grep unzip 查看。
05	处理器	仅支持 X86 操作指令集，暂不支持 ARM 操作指令集。
06	宿主机磁盘空间	用户日志数据挂载盘最小要求 64G，且不能挂载在根路径下；Cent OS 系统/var 目录推荐 15G 以上，/目录推荐 10G 以上。
07	云平台 IO 性能	云平台 IO 性能需要大于等于 $(10*n)$ M/s 的 IO 写入性能，n=检测节点个数。
08	宿主机防火墙	需停止并永久关闭 SELinux 和 Firewall。
09	云 WAF 引流插件	可选，若是选择插件模式部署，则需要在 Nginx/tengine 上集成云 WAF 插件，仅支持 Nginx 1.15.0 及以上版本，tengine 2.3.0 及以上版本。

2.2. 硬件资源要求

深信服云WEB应用防火墙的硬件资源要求如下：

管理节点

逻辑CPU个数	内存	硬盘	对接检测节点个数
2 核	4G	100G	5 个节点
4 核	8G	100G	15 个节点
8 核	16G	100G	50 个节点
12 核	16G	100G	100 个节点

检测节点/单设备部署

逻辑CPU个数	内存	硬盘	应用层吞吐
2 核	4G	100G	25M/50M/100M/200M
4 核	8G	100G	500M
8 核	16G	100G	1G
16 核	32G	100G	2G

2.3. 插件环境要求

由于so插件与nginx以及nginx运行环境都强相关，动态模块.so文件与nginx可执行文件的开发环境与编译配置完全一致时，才可确保两者完全兼容。版本检查与二进制签名是nginx对动态模块.so文件进行兼容性检查的一种安全机制。

云WAF提供了nginx和tengine官方最新的几个版本的so插件库，如果客户刚好使用了这些版本，且是通过在线yum安装，则可以直接使用云WAF提供的so插件库。

如果客户使用的版本不在这里面，或者使用了这里面的版本，但却是通过源码自己编译安装的，这种情况就需要重新编译so插件库，请联系400-630-6430处理。

以下是云WAF提供的so插件库列表：

序号	类型	版本	插件名称
01	Nginx	1.16.1	ngx_1.16.1_http_waf_agent_module.so
02		1.18.0	ngx_1.18.0_http_waf_agent_module.so
03		1.19.10	ngx_1.19.10_http_waf_agent_module.so
04		1.20.1	ngx_1.20.1_http_waf_agent_module.so
05		1.20.2	ngx_1.20.2_http_waf_agent_module.so
06		1.21.1	ngx_1.21.1_http_waf_agent_module.so
07		1.21.3	ngx_1.21.3_http_waf_agent_module.so
08		1.21.5	ngx_1.21.5_http_waf_agent_module.so
09		1.21.6	ngx_1.21.6_http_waf_agent_module.so
10	Tengine	2.3.0	tengine_2.3.0_http_waf_agent_module.so
11		2.3.1	tengine_2.3.1_http_waf_agent_module.so
12		2.3.2	tengine_2.3.2_http_waf_agent_module.so
13		2.3.3	tengine_2.3.3_http_waf_agent_module.so

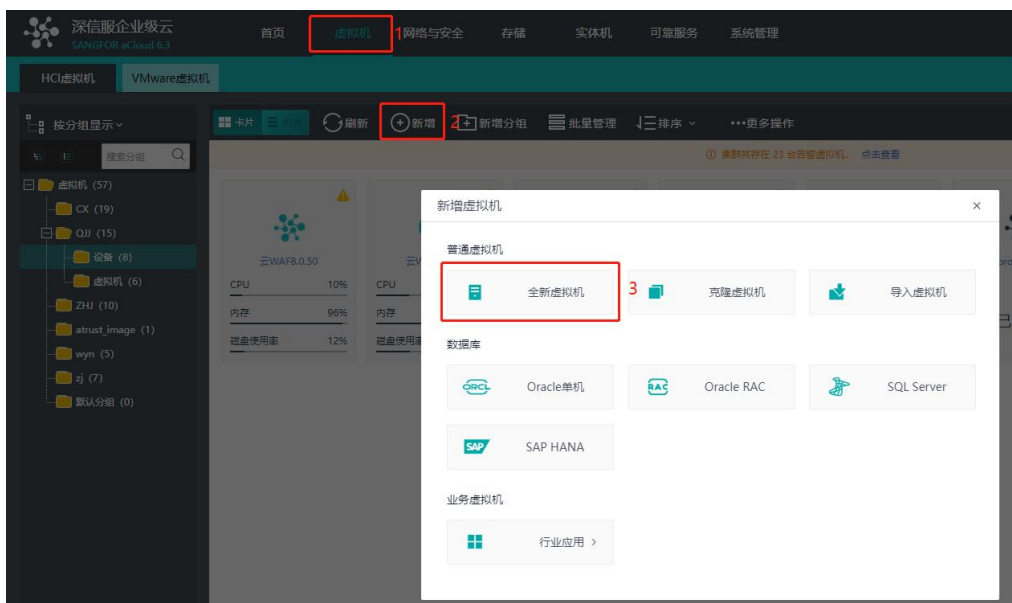
3. 设备部署

3.1. 创建虚拟机

3.1.1. 私有云环境

3.1.1.1. HCI 中创建虚拟机

步骤1. 登录HCI控制台，在[虚拟机]中<新增>虚拟机。



步骤2. 配置虚拟机参数，关键参数选择如下：

- 名称：根据需求自定义；
- 操作系统：选择 CentOS；
- 硬件配置选择：参考 [2.2 章节](#)，最低 2C4G；
- 网卡：启用网卡，选择对应的连接位置。



步骤3. 创建虚拟机完成后，点击<安装系统>进行Cent OS 7系统安装。

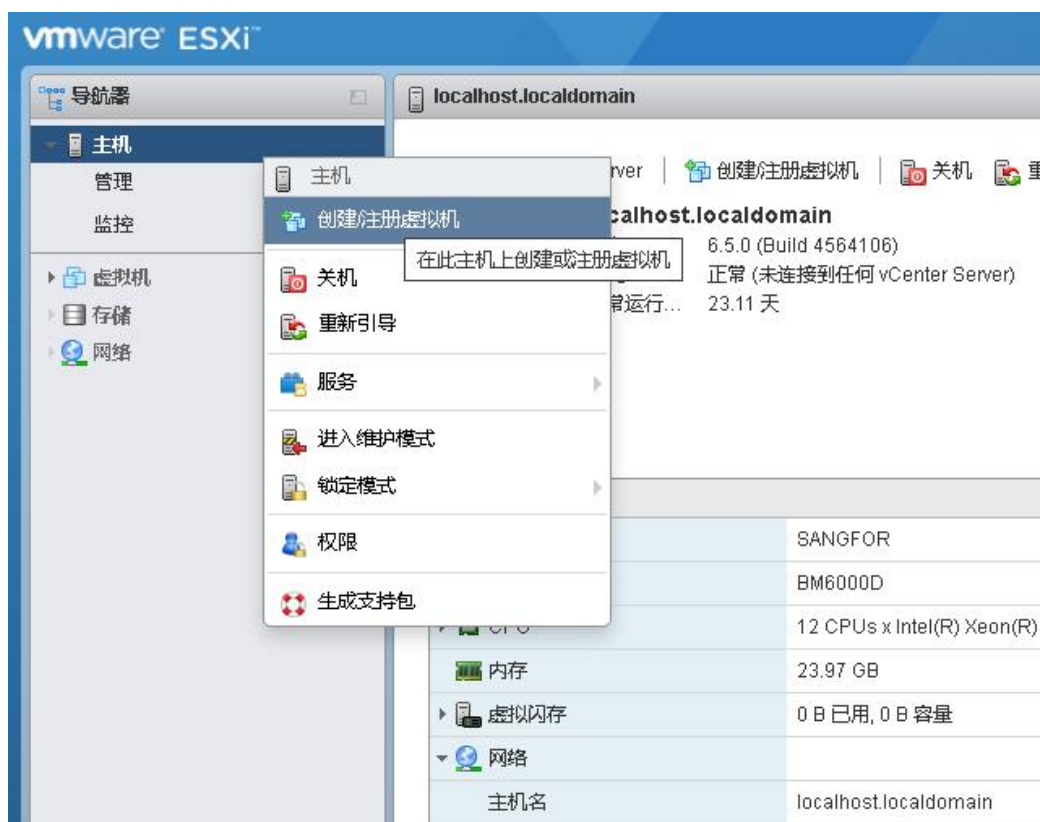


步骤4. 选择从[ISO镜像文件安装/本地上传]上传Cent OS 7镜像后，点击<立即安装>，即可开始安装Cent OS系统，可参考[3.2章节](#)。

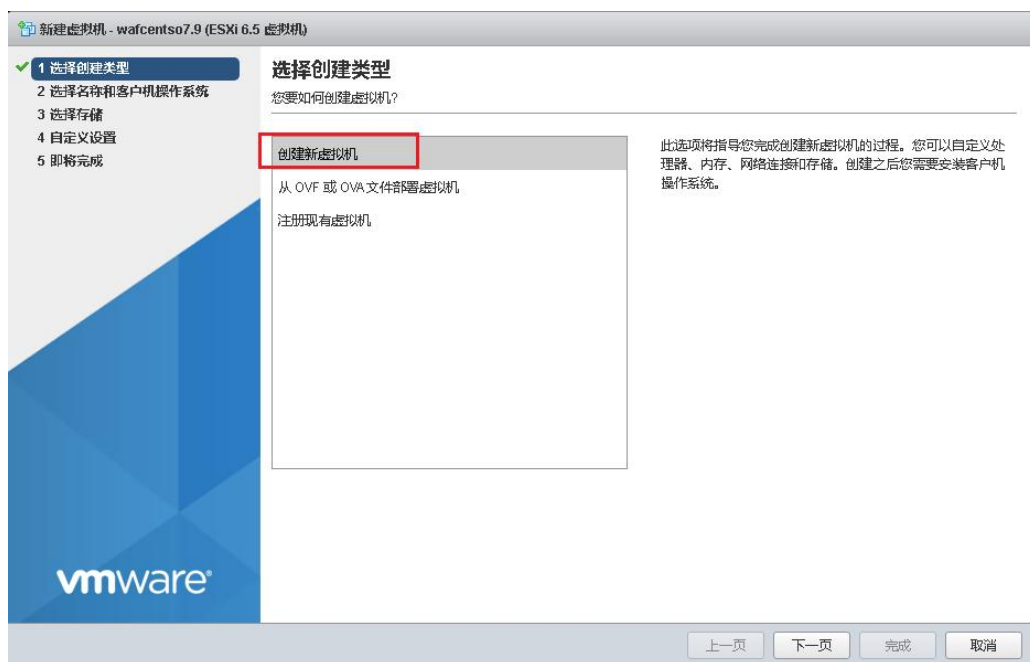


3.1.1.2. VMware ESXI 中创建虚拟机

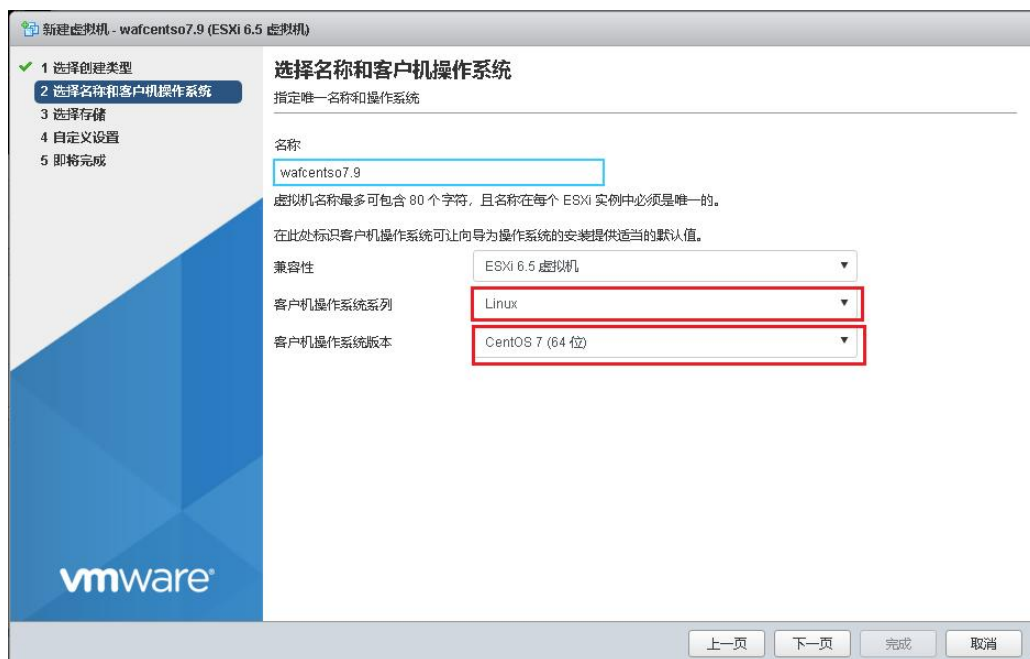
步骤1. 在主机上[创建/注册虚拟机]。



步骤2. 选择创建类型为“创建新虚拟机”。



步骤3. 配置虚拟机的名称与操作系统为Linux、Cent OS 7。



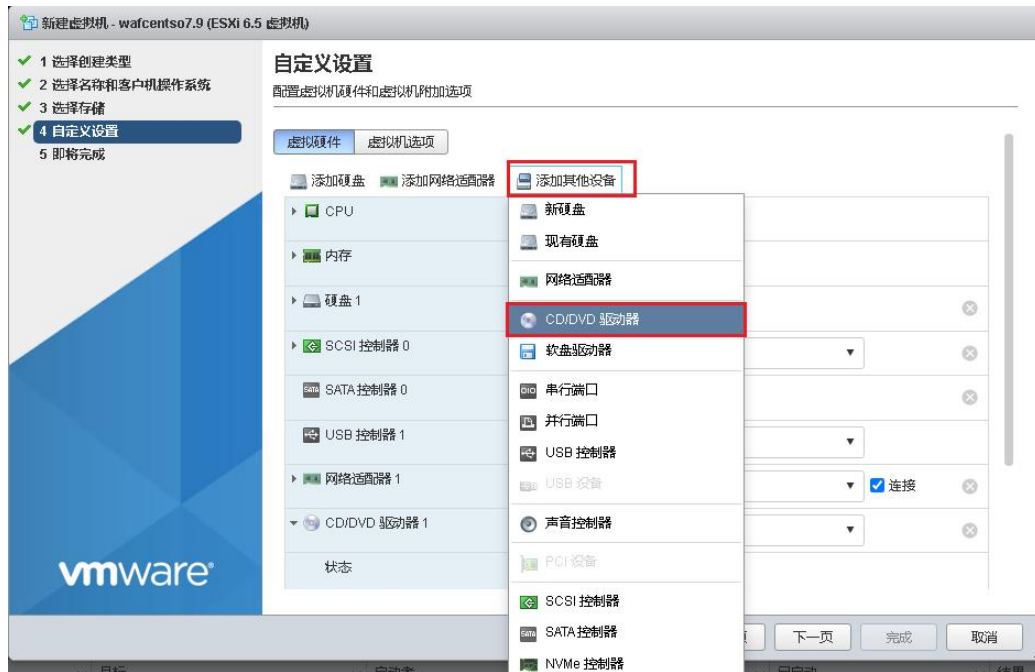
步骤4. 选择虚拟机的存储位置。



步骤5. 配置虚拟机的CPU、内存、磁盘空间，参考[2.2章节](#)，最低2C4G，并配置网卡连接到相应的位置。

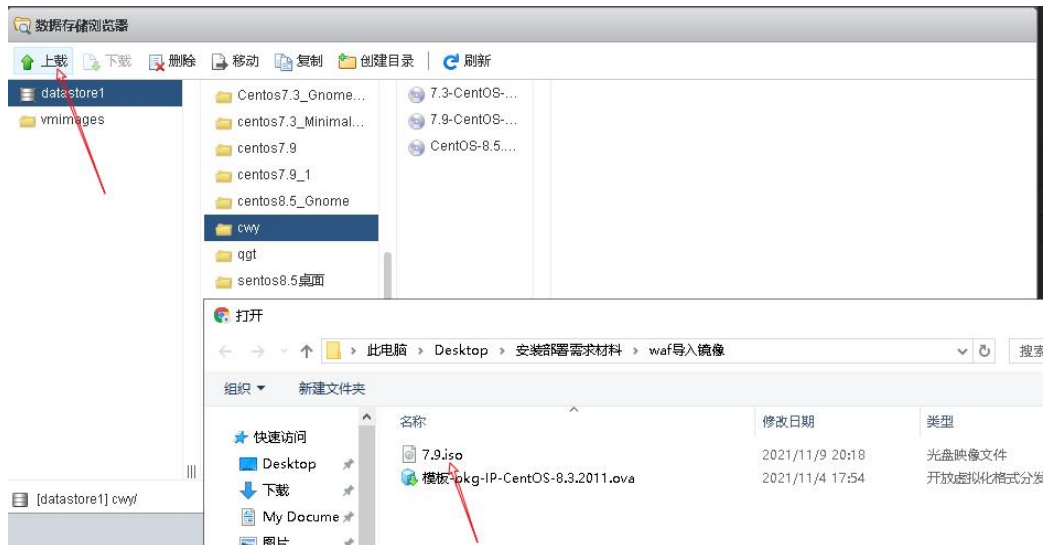


步骤6. 导入Cent OS 7的.iso镜像文件，选择添加其他设备，选择CD/DVD驱动器

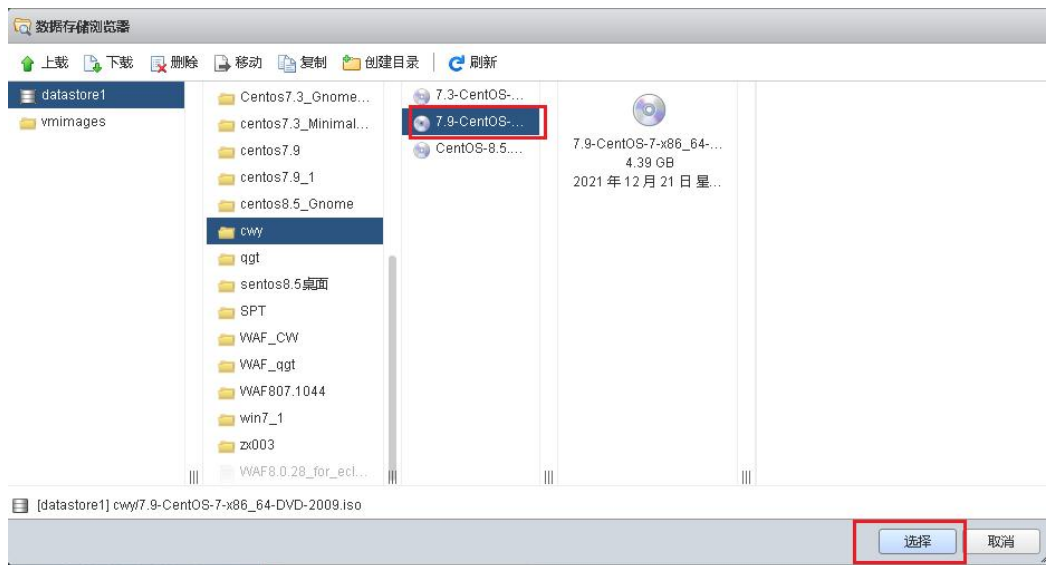


步骤7. 添加CD/DVD驱动器后选择<数据存储ISO文件>，选择存储的位置，并上传Cent OS 7的ISO镜像文件。





步骤8. 文件上传完成后，选择上传的Cent OS7的ISO镜像文件



步骤9. 最后确认配置，点击<完成>，即可完成虚拟机的创建，开始安装Cent OS 7的系统，可参考[3.2章节](#)。



3.1.2. 公有云环境

3.1.2.1. 华为云

步骤1. 注册登录到华为云中，进入[产品/计算/弹性云服务器ECS]中。



步骤2. 点击<立即购买>，跳转购买页面。

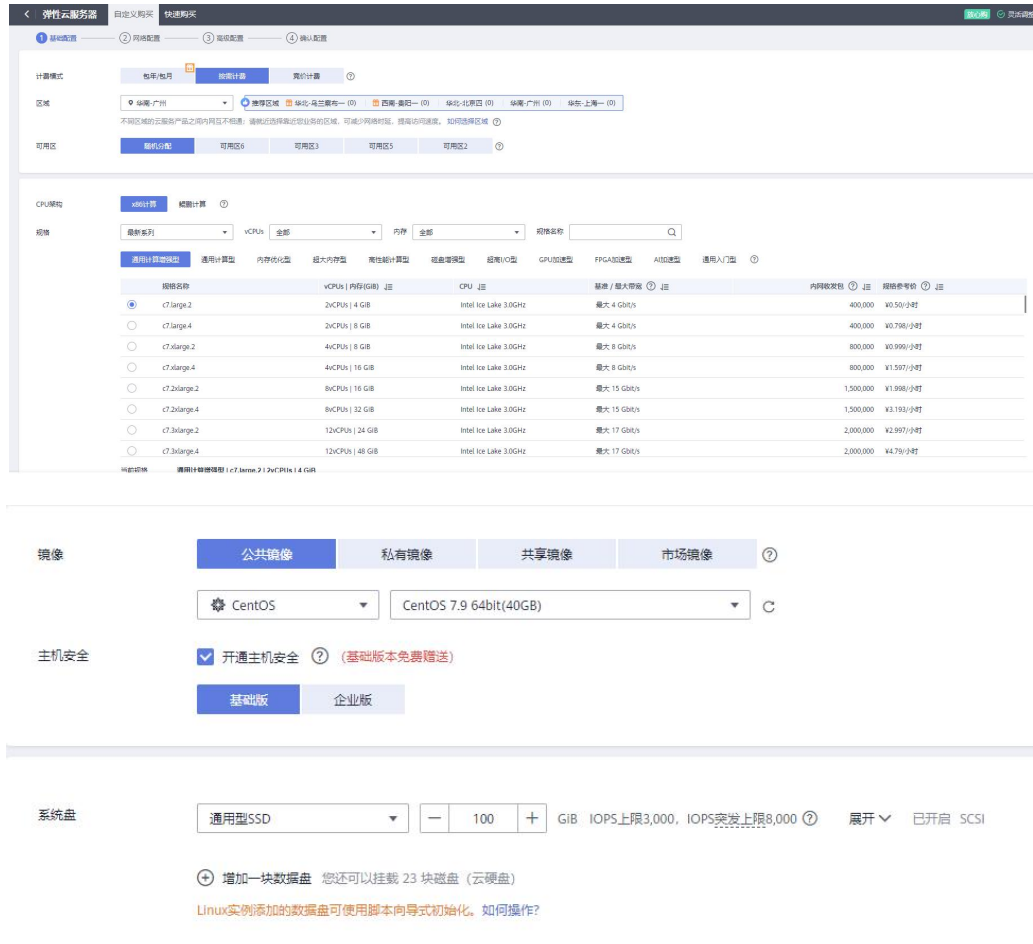


步骤3. 购买ECS服务器，配置购买服务器参数

序号	参数	说明
01	计费模式	<p>计费模式根据业务实际情况购买，例如在测试环境下，仅需部署两三天可以选择按需计费模式，在生产环境部署长期使用可以选择包年/包月模式。</p> <ul style="list-style-type: none"> ● 包年/包月 <p>包年包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。</p> <ul style="list-style-type: none"> ● 按需计费 <p>按需计费是后付费模式，按弹性云服务器的实际使用时长计费，可以随时开通/删除弹性云服务器。</p> <ul style="list-style-type: none"> ● 竞价计费 <p>竞价计费是后付费模式，相较于按需计费模式，以更低的折扣按实际使用时长计费。</p>
02	区域	<p>区域是云服务器的物理数据中心所在的位置，区域不同即云服务器物理数据中心距离用户的物理距离不同，网络延迟不同。为了降低访问时延、提高访问速度，请就近选择靠近您业务的区域。</p>
03	可用区域	<p>可用区是在同一区域下，电力、网络隔离的物理区域，可用区之间网互通，不同可用区之间物理隔离。</p> <p>一个区域内有多个可用区，一个可用区发生故障后不会影响同一区域内的其它可用区。</p>
04	计算架构	<p>部署云 WAF 选择 x86 计算架构。</p> <ul style="list-style-type: none"> ● x86 计算 <p>x86 CPU 架构采用复杂指令集（CISC），CISC 指令集的每个小指令可以执行一些较低阶的硬件操作，指令数目多而且复杂，每条指令的长度并不相同。由于指令执行较为复杂所以每条指令花费的时间较长。</p> <ul style="list-style-type: none"> ● 鲲鹏计算 <p>鲲鹏处理器基于 Arm 结构，采用 RISC 精简指令集（RISC），RISC 是一种执行较少类型计算机指令的微处</p>

		理器，它能够以更快的速度执行操作，使计算机的结构更加简单合理地提高运行速度，相对于 X86 CPU 架构具有更加均衡的性能功耗比。
05	规格	同一实例类型根据 CPU 和内存的配置不同分为多种实例规格，针对不同的应用场景，可以选择不同规格的弹性云服务器。 云 WAF 的 CPU 内存选型可参考 2.2 章节 ，最低 2C4G。
06	镜像	镜像是一个包含了操作系统及必要配置的弹性云服务器模板，使用镜像可以创建弹性云服务器。 部署云 WAF 选择公共镜像-Cent OS-Cent OS 7.9 64bit
07	主机安全	基础版提供账户破解防护，弱口令检测，恶意程序检测等功能，保护云主机基础安全。 企业版提供资产管理，漏洞管理，入侵检测，基线检查，病毒云查杀等功能，满足等保测评要求。 部署云 WAF 无此要求，免费赠送可开启。
08	系统盘	系统盘用于存储云服务器的操作系统，创建云服务器时自带系统盘，且系统盘自动初始化。 部署云 WAF 建议系统盘 100G 以上。
09	网络	虚拟私有云（VPC）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，可以在 VPC 中定义安全组、VPN、IP 地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。提升用户云上资源的安全性，简化用户的网络部署。 不同虚拟私有云里面的弹性云服务器网络默认不通。
10	网卡	网卡是可以绑定到虚拟私有云网络下弹性云服务器上的虚拟网卡。通过网卡，您实现云服务器的网络管理。网卡分为主网卡和扩展网卡。 ● 主网卡 创建云服务器时，随云服务器自动创建的网卡是主网卡。主网卡用于系统的默认路由，不允许删除。 ● 扩展网卡 可以单独创建的网卡是扩展网卡，并支持将其绑定到实例上或从实例上解绑等操作。 部署云 WAF 仅需一个主网卡即可，无需额外的扩展网卡。
11	安全组	安全组类似防火墙功能，是一个逻辑上的分组，用于设置网络访问控制。您可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。 安全组默认出方向放行，并且安全组内的云服务器可以相互访问。 部署云 WAF 建议放通 TCP22（SSH 运维，使用完成后删除放通规则）、TCP4431（Web 控制台）、TCP443（HTTPS 端口用于反向代理 HTTPS 网站）、TCP80 端口（HTTP 端口用于反向代理 HTTP 网站）、TCP20001（检测节点连接管理节点端口）、TCP6970（插件引流端口，若是多核 CPU 则需要放通的端口号从 6970 开始依次递增，一个检测节点有多少核 CPU，就可以配置多少个端口）及其他反向代理需要使用的端口；出方向放通云 WAF 到业务服务器的 IP 及端口。
12	弹性公网 IP	弹性公网 IP 为云服务器提供访问外网的能力，可以灵活绑

		定及解绑，随时修改带宽。未绑定弹性公网 IP 的云服务器无法直接访问外网，无法直接对外进行互通信。 一个弹性公网 IP 只能给一个 ECS 使用，不可以跨区域或跨账号使用，弹性公网 IP 和云服务器必须在同一个区域。 部署云 WAF 建议给云 WAF 的 ECS 单独绑定一个弹性 IP，若部署环境中 NAT 网关等，根据实际环境进行调整。
13	云服务器名称	设置 ECS 服务器的名称。
14	描述	设置 ECS 服务器的描述，可留空。
15	登录凭证	设置 ECS 服务器的后台账号密码。
16	云备份	购买云备份系统会将弹性云服务器绑定至存储库并绑定所选备份策略，定期备份弹性云服务器。 部署云 WAF 可以根据实际情况购买或不购买云备份功能。
17	云服务器组	通过云服务器组功能，弹性云服务器在创建时，将尽量分散地创建在不同的主机上，提高业务的可靠性。
18	高级选项	部署云 WAF 可以根据实际情况配置此功能，也可不配置。



网络 可用私有IP数量: 122个 ⓘ

如需要详细了解私有IP地址，您可前往控制台查看。

扩展网卡 添加一块网卡 您还可以添加 1 块网卡

安全组 ⓘ

安全组是私有IP防火墙功能，是一个逻辑上的分组，用于设置网络访问控制。
 请确保所选安全组已配置了端口 (Linux SSH登录)、3389端口 (Windows远程登录) 和 ICMP 协议 (Ping)。 配置安全组规则

选择安全组规则 ^

[入方向规则](#) [出方向规则](#)

安全组名称	优先级	策略	协议端口	类型	源地址	描述
云WAF	1	允许	TCP: 80	IPv4	0.0.0.0/0	--
	1	允许	TCP: 443	IPv4	0.0.0.0/0	--
	1	允许	TCP: 22	IPv4	0.0.0.0/0	--
	1	允许	TCP: 4431	IPv4	0.0.0.0/0	--
	1	允许	全部	IPv6	云WAF	允许安全组内的弹性云资源接收流量

弹性公网IP 现在购买 使用已有 暂不购买 ⓘ

线路 全动态BGP 静态BGP ⓘ

不低于99.95%可用性保障

公网带宽

按带宽计费 ⓘ

流量较大或较稳定的场景

按流量计费

流量小或流量波动较大场景

加入共享带宽 ⓘ

多业务流量错峰分布场景

指定带宽上限，按实际使用的出公网流量计费，与使用时间无关。

带宽大小 自定义 带宽范围: 1-300 Mbit/s

免费开启DDoS基础防护

释放行为 随实例释放 ⓘ

云服务器名称 允许重名

购买多台云服务器时，支持自动增加数字后缀命名或者自定义规则命名。 ?

描述

0/85

登录凭证

用户名

密码

请牢记密码，如忘记密码可登录ECS控制台重置密码。

确认密码

云备份 ?

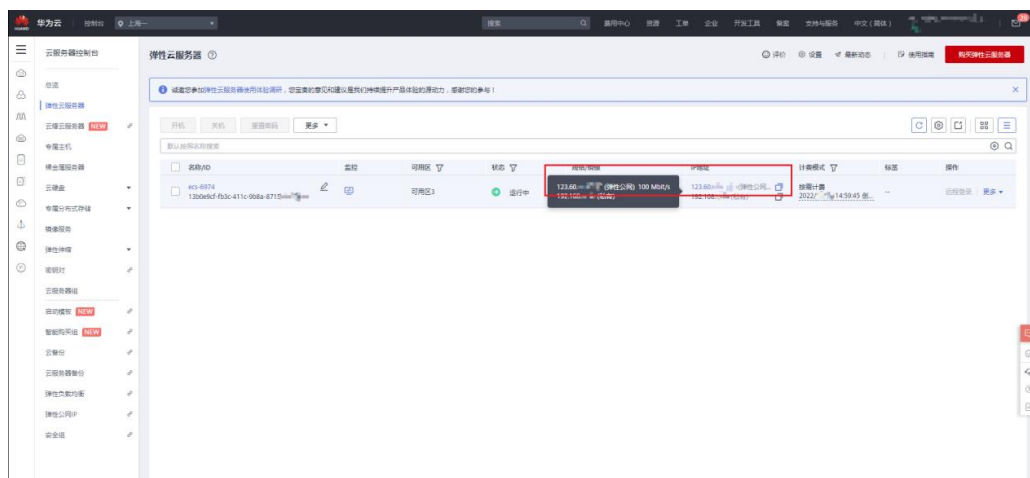
使用云备份服务，需购买备份存储库，存储库是存放服务器产生的备份副本的容器。

云监控 开启详细监控 ?

开启对云服务器CPU，内存，网络，磁盘，进程等指标的1分钟详细监控

云服务器组（可选） ?

步骤4. 创建完成后，在控制台[服务列表/计算/弹性云服务器ECS]中查看创建的云WAF的宿主机服务器，并使用远程工具连接，安装云WAF，可参考[3.3章节](#)。



3.1.2.2. 腾讯云

步骤1. 注册登录到腾讯云中，进入[产品/计算/云服务器]中。



步骤2. 点击<立即选购>，跳转购买页面。



步骤3. 购买云服务器，选择自定义配置，并配置购买服务器参数

序号	参数	说明
01	计费模式	<p>计费模式根据业务实际情况购买，例如在测试环境下，仅需部署两三天可以选择按量计费模式，在生产环境部署长期使用可以选择包年/包月模式。</p> <ul style="list-style-type: none"> ● 包年/包月 <p>包年包月是购买云服务器实例的一种预付费模式，需要一次性支付所选择时间区间的费用，这种模式适用于提前预</p>

		<p>估设备需求量的场景，价格相较于按量计费模式更低廉。</p> <ul style="list-style-type: none"> ● 按量计费 <p>按量计费是购买云服务器实例的一种后付费模式，不需要提前支付费用，但需要冻结一定的费用，可以随时开通/销毁云服务器，按实例的实际使用量付费，计费时间粒度精确到秒，每小时整点进行一次结算，价格比包年包月计费模式高 3-4 倍。</p> <ul style="list-style-type: none"> ● 竞价实例 <p>竞价实例是类似按量付费模式的一种后付费模式（按秒计费，整点结算），与按量付费相比，竞价实例采用市场浮动计费，同时会因为资源库存减少、其他用户出价竞争而发生系统主动回收实例的情况。与稳定性下降所对应的，竞价实例相比按量付费会有较大幅度优惠，一般价格区间为后者的 10%~20%。</p>
02	区域	<p>腾讯云云服务器托管机房分布在全球多个位置，由不同的地域（region）构成。每个地域（region）都指一个独立的物理数据中心，不同地域间的云服务器内网不互通。</p> <p>选择最靠近您客户的地域，可降低访问时延，创建成功后不支持切换地域。</p>
03	可用区域	<p>每个地域内都有多个物理上相互隔离的位置，称为可用区（zone）。每个可用区都是独立的，同一地域下的可用区通过低时延的内网链路相连。同一地域下的不同可用区间的云服务器可以通过内网互相访问。</p>
04	网络	<p>虚拟私有云（VPC）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，可以在 VPC 中定义安全组、VPN、IP 地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。提升用户云上资源的安全性，简化用户的网络部署。</p> <p>不同虚拟私有云里面的弹性云服务器网络默认不通。</p>
05	实例	<p>腾讯云目前提供了不同的实例族，包含标准型，内存型，高 IO 型，计算型，异构计算型等，每种实例族下有不同的实例类型，不同的实例族都有不同的性能，为获得最佳性能，建议在新建实例时使用最新一代实例类型。</p> <p>云 WAF 的 CPU 内存选型可参考 2.2 章节，最低 2C4G。</p>
06	镜像	<p>镜像是一个包含了操作系统及必要配置的弹性云服务器模板，使用镜像可以创建弹性云服务器。</p> <p>部署云 WAF 选择公共镜像-Cent OS-Cent OS 7.9 64bit</p>
07	系统盘	<p>系统盘用于存储云服务器的操作系统，创建云服务器时自带系统盘，且系统盘自动初始化。</p> <p>部署云 WAF 建议系统盘 100G 以上。</p>
08	定期快照	<p>快照可恢复由用户误删，病毒感染等情况导致的数据异常。</p> <p>部署云 WAF 可以根据实际情况购买或不购买快照功能。</p>
09	公网带宽	<p>云服务器需要外网访问能力的时候，需要为云服务器分配公网 IP，如果云服务器不分配公网 IP，不支持外出流量，并且无法使用外网 IP 对外进行互相通信。</p> <p>部署云 WAF 建议给云 WAF 的 ECS 单独绑定一个弹性 IP，若部署环境中 NAT 网关等，根据实际环境进行调整。</p>

10	IPv6 地址	腾讯云目前 IPv6/IPv4 双栈 VPC 功能处于内测中，如有需要，需要提交内测申请，具体可参考腾讯云官方文档开通 IPv6 相关功能，并部署在支持 IPv6 环境的 VPC 网络中。 https://cloud.tencent.com/document/product/1142/47665 云 WAF 支持 IPv6 的反向代理及防护。
11	安全组	安全组是一种有状态的包过滤虚拟防火墙，用于设置单台或多台云服务器的网络访问控制，安全组是一个逻辑上的分组，是重要的网络安全隔离手段，用户可以将同一地域内具有相同网络安全隔离需求的基础网络云服务器或弹性网卡实例加到同一个安全组内。 部署云 WAF 建议放通 TCP22（SSH 运维，使用完成后删除放通规则）、TCP4431（Web 控制台）、TCP443（HTTPS 端口用于反向代理 HTTPS 网站）、TCP80 端口（HTTP 端口用于反向代理 HTTP 网站）、TCP20001（检测节点连接管理节点端口）、TCP6970（插件引流端口，若是多核 CPU 则需要放通的端口号从 6970 开始依次递增，一个检测节点有多少核 CPU，就可以配置多少个端口）及其他反向代理需要使用的端口；出方向放通云 WAF 到业务服务器的 IP 及端口。
12	所属项目	项目为一个虚拟概念，用户可以在一个账户下面建立多个项目，每个项目中管理不同的云服务器，并且针对不同子账号设置不同的项目权限。
13	标签	标签是一个键-值对(Key-Value)，您可以通过对云服务器设置标签实现资源的分类管理。通过标签，可以非常方便筛选过滤出对应的资源，进行操作
14	实例名称	设置云服务器的名称。
15	登录方式	设置云服务器的后台账号密码。
16	安全加固	免费开通 DDoS 防护和主机安全基础版 基于腾讯安全积累的海量威胁数据，利用机器学习为用户提供资产管理、木马文件查杀、黑客入侵检测、漏洞风险预警及安全基线等安全防护服务，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系。 CVM 默认安装基础版，仅提供密码破解检测、异常登录提醒等基础功能，建议用户购买升级主机安全专业版，获得更多安全防护。 部署云 WAF 可以根据实际情况购买或不购买安全加固功能。
17	自动化助手	自动化助手（TencentCloud Automation Tools, TAT）是云服务器 CVM 和轻量应用服务器 Lighthouse 的原生运维部署工具。自动化助手提供了一种自动化的远程操作方式，无需登录及密码，即可批量执行命令（Shell、PowerShell 及 Python 等），完成运行自动化运维脚本、轮询进程、安装/卸载软件、更新应用及安装补丁等任务。 部署云 WAF 可以根据实际情况勾选或不勾选自动化助手功能。
18	定时销毁	开启定时销毁后，系统将在设定的时间点自动销毁机器，销毁后所有数据将被清除且不可恢复，请提前备份数据。 部署云 WAF 可以根据实际情况选择是否设置定时销毁功能。

19	高级设置	部署云 WAF 可以根据实际情况配置此功能，也可不配置。
----	------	------------------------------

1.选择机型 2.设置主机 3.确认配置信息

计费模式

包年包月
按量计费
竞价实例
① 详细对比

地域

华南地区
华东地区
华北地区
西南地区
港澳台地区

广州
上海
南京
北京
成都
重庆
中国香港

亚太东南
亚太南部
亚太东北
美国西部
美国东部

新加坡
曼谷
雅加达
NEW
孟买
首尔
东京
硅谷
弗吉尼亚

北美地区
欧洲地区
南美地区

多伦多
法兰克福
莫斯科
圣保罗
NEW
① 更多地域

不同地域云产品之间内网不互通；选择最靠近您客户的地域，可降低访问时延，创建成功后不支持切换地域。 [查看我的云服务商地域](#) [详细对比](#)

可用区

随机可用区
南京一区
南京二区
南京三区
①

网络

Default-VPC (默认)
Default-Subnet (默认)
①
② 子网剩余可用IP 4093个

当前网络为默认私有网络/子网，建议您根据业务需要进行调整
 如果有私有网络/子网不符合您的要求，可以去控制台 [新建私有网络](#) 或 [新建子网](#)。云服务器购买后可以通过控制台切换私有网络完成私有网络/子网的切换

实例

2核
4GB

全部机型
标准型
高IO型
内存型
计算型
GPU机型
FPGA机型
大数据型
黑石物理服务器2.0
①

全部实例类型
标准型S6
标准型SA2
标准型S5
NEW
标准存储增强型S5se
NEW
标准型SA3
NEW
标准型SR4
NEW
标准型S4

标准网络优化型SN3ne
标准型S3
标准型SA1
标准型S2
标准型S1
高IO型IT5
NEW
高IO型IT3
高IO型I3

内存型M6
内存型MA3
内存型MA2
内存型M5
NEW
内存型M4
内存型M3
内存型M2
内存型M1
计算型C6

计算型C5
计算型C4
计算网络增强型CN3
计算型C3
计算型C2
GPU计算型GN6
GPU计算型GN6S
GPU计算型GN7

镜像

公共镜像
自定义镜像
共享镜像
镜像市场
①

CentOS
64位
CentOS 7.9 64位
①

系统盘

高性能云硬盘
- 100 + GB
①
② 选购指引

购买成功后，系统盘不支持更换介质

数据盘

+ 新建云硬盘数据盘 还可增加20块数据盘 ②

定期快照

对系统盘设置定期快照
default-policy 星期四...12:00(保留30天后自动删除)
①

对数据盘设置定期快照
default-policy 星期四...12:00(保留30天后自动删除)
①

推荐 快照可恢复由用户误删，病毒感染等情况导致的数据异常，目前中国境内每个地域提供 50GB 免费额度，详情可见 [快照计费概述](#)

公网带宽

免费分配独立公网IP
①

按带宽计费
按使用流量
①
② 详细对比

5
Mbps
①

注意：流量费用每小时结算一次，当账户余额不足时，两小时内将被停止流量服务。

IPv6地址

所选的VPC/子网未开通IPv6 [去开通](#)

文档版本 01（2022-08-16）

28

1.选择机型 **2.设置主机** 3.确认配置信息

安全组 ② [使用指引](#)

请选择安全组

如您有业务需要放通其他端口，您可以 [新建安全组](#)

所属项目 ②

标签 ①

标签键	标签值	操作
<input type="text" value="可选，请选择一个标签键"/>	<input type="text" value="可选，请选择标签值"/>	删除

[添加](#)

如有标签/标签值不符合您的要求，可以去控制台 [新建标签/标签值](#)

实例名称 支持批量连续命名或指定模式串命名，最多126个字符，您还可以输入126个字符 ①

登录方式 ②

注：请牢记您所设置的密码，如遗忘可登录CVM控制台重置密码。自定义密码的实例不支持保存为自动模板。

用户名 root

密码

确认密码

安全加固 免费开通 ②
安装组件免费开通DDoS防护和主机安全基础版 [详细介绍](#)

云监控 免费开通 ②
免费开通云产品监控、分析和实施告警，安装组件获取主机监控指标 [详细介绍](#)

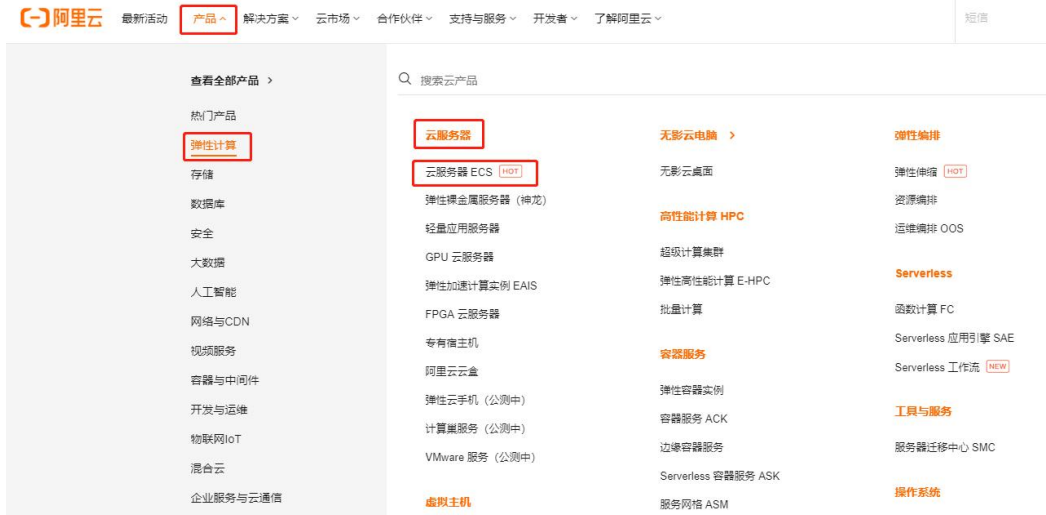
自动化助手 免费开通 **NEW**
安装组件免费开通自动化助手，免密码、免SSH登录即可批量管理实例、执行命令，完成日常管理任务 [详细介绍](#)

定时销毁 开启定时销毁 ②
开启定时销毁后，系统将在设定时间点自动销毁机器

▶ [高级设置](#)

3.1.2.3. 阿里云

步骤1. 注册登录到阿里云中，进入[产品/弹性计算/云服务器/云服务器ECS]中。



步骤2. 点击<立即购买>，跳转购买页面。



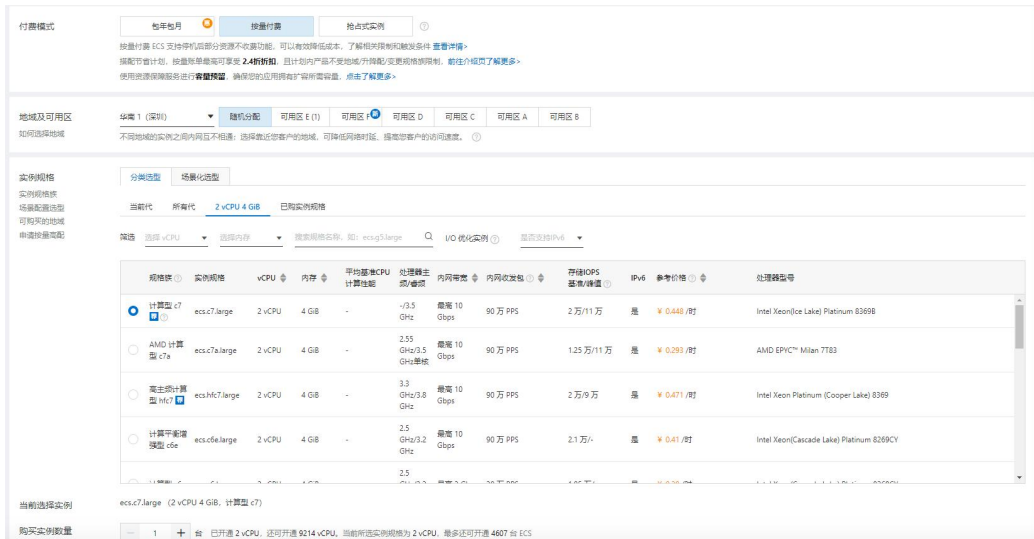
步骤3. 购买ECS服务器，配置购买服务器参数

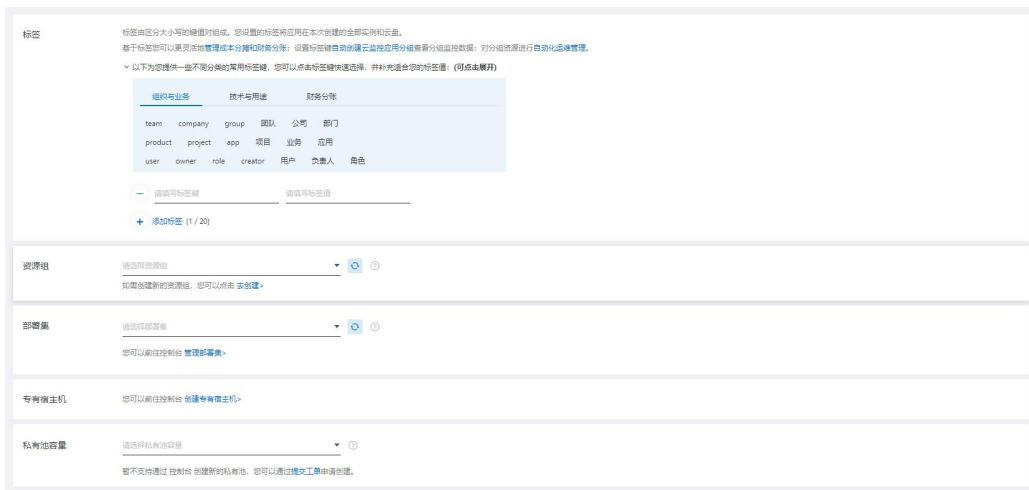
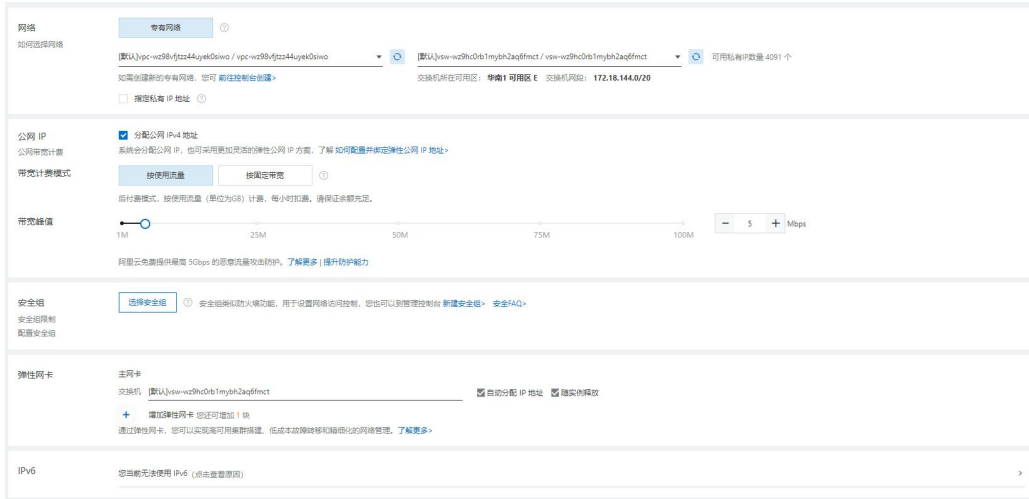
序号	参数	说明
01	计费模式	<p>计费模式根据业务实际情况购买，例如在测试环境下，仅需部署两三天可以选择按需计费模式，在生产环境部署长期使用可以选择包年/包月模式。</p> <ul style="list-style-type: none"> ● 包年包月 按月购买及续费，为预付费模式。若购买中国内地地域的 ECS 用于网站 Web 访问，请及时备案。若 ECS 用于 SLB，请前往 SLB 新购页面购买带宽，ECS 仅需保留少量带宽以便您管理。 ● 按量付费 按实际开通时长以小时为单位进行收费，后付费模式。按量付费 ECS 不支持备案服务。 ● 抢占式实例 相对于按量付费实例价格有一定的折扣，价格随供求波动，按实际使用时长进行收费，后付费模式。您愿意支付

		每小时的实例最高价。当您的出价高于当前市场成交价时，您的实例就会运行。阿里云会根据供需资源或市场成交价的变化释放您的抢占式实例。抢占式实例不支持备案服务。
02	地域及可用区	<ul style="list-style-type: none"> ● 地域 地域指的是 ECS 实例所在的物理位置。 ● 可用区 可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。 如果您的应用需要较高的容灾能力，建议您将云服务器 ECS 实例部署在同一地域的不同可用区内。 如果您的应用在实例之间需要较低的网络时延，则建议您将 ECS 实例创建在相同的可用区内。
03	实例规格	同一实例类型根据 CPU 和内存的配置不同分为多种实例规格，针对不同的应用场景，可以选择不同规格的弹性云服务器。 云 WAF 的 CPU 内存选型可参考 硬件资源要求 2.2 章节 ，最低 2C4G，部署云 WAF 选择 x86 计算架构。
04	购买实例数量	根据实际需求选择购买云服务器的数量。
05	镜像	<p>镜像是一个包含了操作系统及必要配置的弹性云服务器模板，使用镜像可以创建弹性云服务器。</p> <p>部署云 WAF 选择公共镜像-Cent OS-Cent OS 7.9 64bit</p> <ul style="list-style-type: none"> ● 安全加固 云服务器加载基础安全组件，提供网站漏洞检查、云产品安全配置检查、主机登录异常告警等安全功能，并可以通过云安全中心统一管理。 部署云 WAF 无此要求，免费赠送可开启。 ● 可信系统 可信系统检查并报告系统启动链中 UEFI、GRUB 等各组件的完整性，还可以帮助您监控您指定应用加载启动情况。 部署云 WAF 无此要求，免费赠送可开启。
06	系统盘	<p>系统盘用于存储云服务器的操作系统，创建云服务器时自带系统盘，且系统盘自动初始化。</p> <p>部署云 WAF 建议系统盘 100G 以上。</p>
07	快照服务	<p>快照服务能定时对云盘进行备份。可应对病毒感染、数据误删等风险。</p> <p>部署云 WAF 可以根据实际情况购买或不购买快照功能。</p>
08	网络	<ul style="list-style-type: none"> ● 专有网络 专有网络（Virtual Private Cloud，简称 VPC）是您基于阿里云构建的一个隔离的网络环境，专有网络之间逻辑上彻底隔离。您可以自定义这个专有网络的拓扑和 IP 地址，适用于对网络安全性要求较高和有一定网络管理能力的用户。 ● 经典网络 经典网络类型的云产品，统一部署在阿里云公共基础设施内，规划和管理由阿里云负责，更适合对网络易用性要求比较高的用户。

09	公网 IP	<p>弹性公网 IP（Elastic IP Address，简称 EIP）是可以独立购买和持有的公网 IP 地址资源。目前，EIP 支持绑定到专有网络类型的 ECS 实例、专有网络类型的私网 SLB 实例、专有网络类型的辅助弹性网卡、NAT 网关和高可用虚拟 IP 上。</p> <p>EIP 是一种 NAT IP，它实际位于阿里云的公网网关上，通过 NAT 方式映射到被绑定的云资源上。当 EIP 和云资源绑定后，云资源可以通过 EIP 与公网通信。</p> <ul style="list-style-type: none"> ● 按固定带宽 <p>需指定公网出方向的带宽的大小，如 10Mbps，适用于业务场景对于网络带宽要求比较稳定的客户，费用较低。带宽费用合并并在 ECS 实例中收取。</p> <ul style="list-style-type: none"> ● 按使用流量 <p>是按公网出方向的实际发生的网络流量进行收费，适用于业务场景对网络带宽需求变化较大的场景，如平时带宽使用较低但间歇性的出现网络访问高峰的场景；为了防止突然爆发的流量产生较高的费用，可以指定容许的最大网络带宽进行限制。后付费模式，按使用流量（单位为 GB）计费，每小时扣费。请保证余额充足。</p> <p>部署云 WAF 建议给云 WAF 的 ECS 单独绑定一个弹性 IP，若部署环境中 NAT 网关等，根据实际环境进行调整。</p>
10	安全组	<p>安全组类似防火墙功能，是一个逻辑上的分组，用于设置网络访问控制。您可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。</p> <p>安全组默认出方向放行，并且安全组内的云服务器可以相互访问。</p> <p>部署云 WAF 建议放通 TCP22（SSH 运维，使用完成后删除放通规则）、TCP4431（Web 控制台）、TCP443（HTTPS 端口用于反向代理 HTTPS 网站）、TCP80 端口（HTTP 端口用于反向代理 HTTP 网站）、TCP20001（检测节点连接管理节点端口）、TCP6970（插件引流端口，若是多核 CPU 则需要放通的端口号从 6970 开始依次递增，一个检测节点有多少核 CPU，就可以配置多少个端口）及其他反向代理需要使用的端口；出方向放通云 WAF 到业务服务器的 IP 及端口。</p>
11	弹性网卡	<p>弹性网卡 ENI（Elastic Network Interface）是一种可以绑定到专有网络 VPC 类型 ECS 实例上的虚拟网卡。通过弹性网卡，您可以实现高可用集群搭建、低成本故障转移和精细化的网络管理。</p> <p>部署云 WAF 仅需一个主网卡即可，无需额外的辅助网卡。</p>
12	IPv6	<p>阿里云使用 IPv6 功能需要将云服务器部署在支持 IPv6 的地区中，连接的虚拟交换机开启 IPv6 的功能。具体可参考 https://help.aliyun.com/product/85563.html。</p> <p>云 WAF 支持 IPv6 的反向代理及防护。</p>
13	登录凭证	设置 ECS 服务器的后台账号密码。
14	实例名称	设置 ECS 服务器的名称。
15	描述	设置 ECS 服务器的描述，可留空。
16	主机名	表示操作系统内部的计算机名。

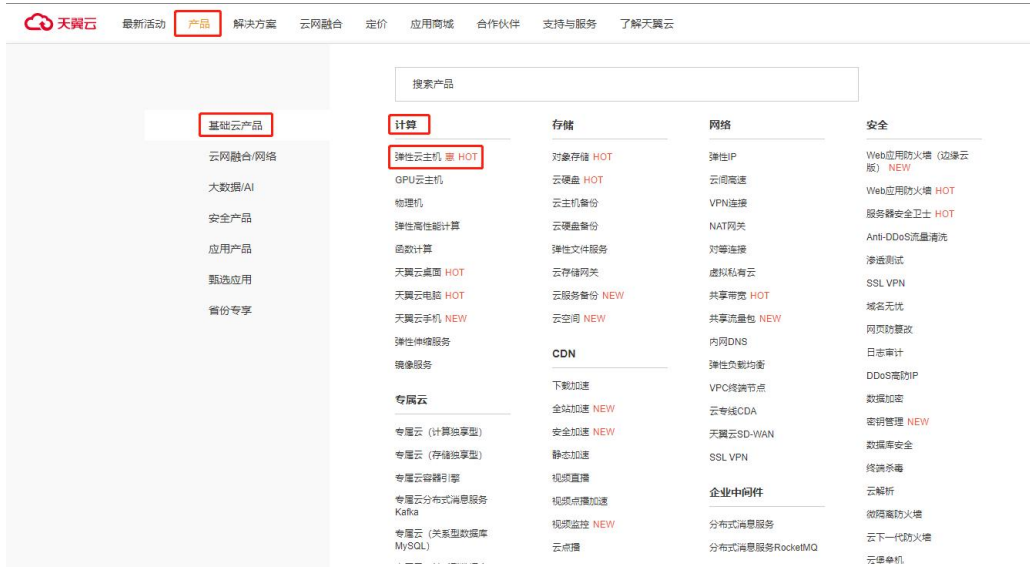
17	有序后缀	为实例名称和主机名添加有序后缀。 部署云 WAF 可以根据实际情况勾选或不勾选此功能。
18	实例释放保护	防止通过控制台或 API 误删除释放。 部署云 WAF 可以根据实际情况勾选或不勾选此功能。
19	高级选项	部署云 WAF 可以根据实际情况配置此功能，也可不配置。
20	标签	基于标签您可以更灵活地管理成本分摊和财务分账；设置标签键自动创建云监控应用分组查看分组监控数据；对分组资源进行自动化运维管理。 部署云 WAF 可以根据实际情况配置此功能，也可不配置。
21	资源组	在单个云账号下将一组相关资源进行统一管理的容器，一个资源只能归属于一个资源组。根据不同的业务场景，您可以将资源组映射为项目、应用或组织等概念。 部署云 WAF 可以根据实际情况配置此功能，也可不配置。
22	部署集	在指定部署集中创建 ECS 实例时，会和处于同一部署集中的其他 ECS 实例严格按物理服务器打散，保障在硬件故障等异常情况下的服务高可用性。 部署云 WAF 可以根据实际情况配置此功能，也可不配置。
23	专有宿主机	阿里云专有宿主机（Dedicated Host，简称 DDH）是阿里云专为企业客户定制优化的解决方案，具有物理资源独享、部署更灵活、配置更丰富、性价比更高等特点，可以有效地降低企业上云的 TCO。 部署云 WAF 可以根据实际情况配置此功能，也可不配置。
24	私有池容量	购买弹性保障或立即生效容量预定后，阿里云以私有池的方式预留属性一致的资源。 部署云 WAF 可以根据实际情况配置此功能，也可不配置。





3.1.2.4. 天翼云

步骤1. 注册登录到天翼云中，进入[产品/基础云计算产品/计算/弹性云服务器]中。



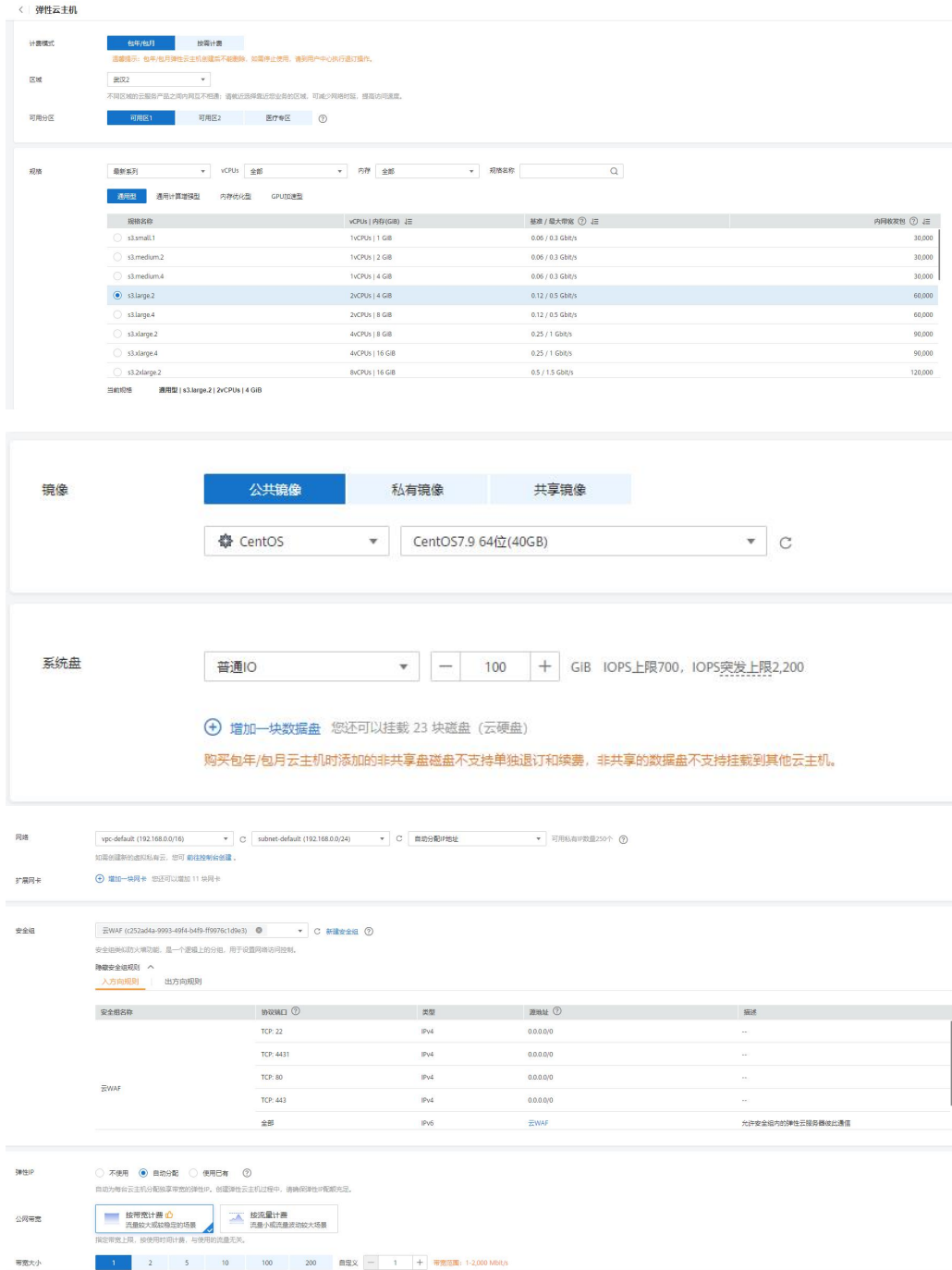
步骤2. 点击<立即开通>，跳转购买页面。



步骤3. 购买弹性云服务器，配置购买服务器参数

序号	参数	说明
01	计费模式	<p>计费模式根据业务实际情况购买，例如在测试环境下，仅需部署两三天可以选择按需计费模式，在生产环境部署长期使用可以选择包年/包月模式。</p> <ul style="list-style-type: none"> ● 包年/包月 <p>包年包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。</p> <ul style="list-style-type: none"> ● 按需计费 <p>按需计费是后付费模式，按弹性云服务器的实际使用时长计费，可以随时开通/删除弹性云服务器。</p>
02	区域	不同区域的云服务产品之间内网互不相通；请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。
03	可用区域	指在同一地域下，电力、网络隔离的物理区域，可用分区

		之间内网互通，不同可用分区之间物理隔离。如果您需要提高应用的高可用性，建议您将云主机创建在不同的可用分区内。
04	规格	同一实例类型根据 CPU 和内存的配置不同分为多种实例规格，针对不同的应用场景，可以选择不同规格的弹性云服务器。 云 WAF 的 CPU 内存选型可参考 2.2 章节 ，最低 2C4G。
05	镜像	镜像是一个包含了操作系统及必要配置的弹性云服务器模板，使用镜像可以创建弹性云服务器。 部署云 WAF 选择公共镜像-Cent OS-Cent OS 7.9 64bit
06	系统盘	系统盘用于存储云服务器的操作系统，创建云服务器时自带系统盘，且系统盘自动初始化。 部署云 WAF 建议系统盘 100G 以上。
07	网络	虚拟私有云可以方便的管理、配置内部网络，进行安全、快捷的网络变更，不同虚拟私有云里面的云主机网络默认不通。
08	扩展网卡	部署云 WAF 仅需一个主网卡即可，无需额外的扩展网卡。
09	安全组	安全组类似防火墙功能，是一个逻辑上的分组，用于设置网络访问控制。您可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。 安全组默认出方向放行，并且安全组内的云服务器可以相互访问。 部署云 WAF 建议放通 TCP22（SSH 运维，使用完成后再删除放通规则）、TCP4431（Web 控制台）、TCP443（HTTPS 端口用于反向代理 HTTPS 网站）、TCP80 端口（HTTP 端口用于反向代理 HTTP 网站）、TCP20001（检测节点连接管理节点端口）、TCP6970（插件引流端口，若是多核 CPU 则需要放通的端口号从 6970 开始依次递增，一个检测节点有多少核 CPU，就可以配置多少个端口）及其他反向代理需要使用的端口；出方向放通云 WAF 到业务服务器的 IP 及端口。
10	弹性公网 IP	弹性公网 IP 为云服务器提供访问外网的能力，可以灵活绑定及解绑，随时修改带宽。未绑定弹性公网 IP 的云服务器无法直接访问外网，无法直接对外进行互相通信。 一个弹性公网 IP 只能给一个云服务器使用，不可以跨区域或跨账号使用，弹性公网 IP 和云服务器必须在同一个区域。 部署云 WAF 建议给云 WAF 的云服务器单独绑定一个弹性 IP，若部署环境中存在 NAT 网关等，根据实际环境进行调整。
11	云服务器名称	设置 ECS 服务器的名称。
12	登录凭证	设置 ECS 服务器的后台账号密码。
13	云服务器组	通过云服务器组功能，弹性云服务器在创建时，将尽量分散地创建在不同的主机上，提高业务的可靠性。
14	高级选项	部署云 WAF 可以根据实际情况配置此功能，也可不配置。



云主机名称

购买多台云主机时，名称自动按序增加4位数字后缀。例如：输入ecs，从ecs-0001开始命名；若已有ecs-0010，从ecs-0011开始命名。

登录方式

用户名 root

密码 请妥善保管密码，系统无法获取您设置的密码内容。

确认密码

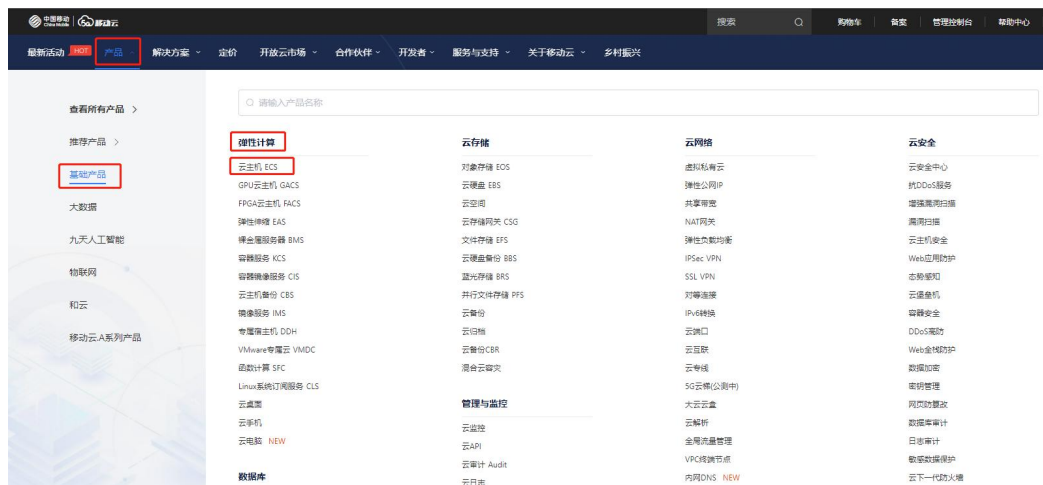
云主机组（可选）

[查看云主机组](#)

高级选项 现在配置

3.1.2.5. 移动云

步骤1. 注册登录到移动云中，进入[产品/基础产品/弹性计算/云主机ECS]中。



步骤2. 点击<立即订购>，跳转购买页面。



产品类型

通用型 内存型 计算型 大数据型 异构加速计算型

步骤3. 购买ECS服务器，配置购买服务器参数

序号	参数	说明
01	计费模式	<p>计费模式根据业务实际情况购买，例如在测试环境下，仅需部署两三天可以选择按时计费模式，在生产环境部署长期使用可以选择按年计费模式。</p> <ul style="list-style-type: none"> ● 按年计费 <p>包年云主机一次性支付全部费用，资源期限未满，不支持退订与退费。</p> <ul style="list-style-type: none"> ● 按月计费 <p>按月计费的云主机，不会自动续订，如有需要，可在控制台或订购确认页面选择自动续订。</p> <ul style="list-style-type: none"> ● 按时计费 <p>按时计费会在每个月底根据您的使用情况给您提供话单，需要提前充值。</p>
02	地域	不同地域的实例之间内网互不相通；选择靠近您的地域，可降低网络时延、提高您的访问速度。
03	架构	<p>部署云 WAF 选择 x86 计算架构。</p> <ul style="list-style-type: none"> ● x86 计算 <p>x86 CPU 架构采用复杂指令集（CISC），CISC 指令集的每个小指令可以执行一些较低阶的硬件操作，指令数目多而且复杂，每条指令的长度并不相同。由于指令执行较为复杂所以每条指令花费的时间较长。</p>
04	分类	<p>不同类型的主机适用的场景不同。</p> <p>部署云 WAF 选择通用性即可。</p>
05	规格	<p>同一实例类型根据 CPU 和内存的配置不同分为多种实例规格，针对不同的应用场景，可以选择不同规格的弹性云服务器。</p> <p>云 WAF 的 CPU 内存选型可参考 2.2 章节，最低 2C4G。</p>
06	镜像	镜像是一个包含了操作系统及必要配置的弹性云服务器模板，使用镜像可以创建弹性云服务器。

		<p>部署云 WAF 选择公共镜像-Cent OS-Cent OS 7.9 64bit</p> <ul style="list-style-type: none"> ● 安全加固 <p>云服务器加载基础安全组件，提供系统漏洞检测、暴力破解检测、主机登录异常告警等基础安全功能，如需使用云安全中心高级版功能，请进入云安全中心进行升级或授权。</p> <p>部署云 WAF 无此要求，免费赠送可开启。</p>
07	系统盘	<p>系统盘用于存储云服务器的操作系统，创建云服务器时自带系统盘，且系统盘自动初始化。</p> <p>部署云 WAF 建议系统盘 100G 以上。</p>
08	网络	<p>虚拟私有云（VPC）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，可以在 VPC 中定义安全组、VPN、IP 地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。提升用户云上资源的安全性，简化用户的网络部署。</p> <p>不同虚拟私有云里面的弹性云服务器网络默认不通。</p> <p>网卡选择默认网卡即可。</p>
09	公网 IP	<p>弹性公网 IP 为云服务器提供访问外网的能力，可以灵活绑定及解绑，随时修改带宽。未绑定弹性公网 IP 的云服务器无法直接访问外网，无法直接对外进行互相通信。</p> <p>一个弹性公网 IP 只能给一个 ECS 使用，不可以跨区域或跨账号使用，弹性公网 IP 和云服务器必须在同一个区域。</p> <p>部署云 WAF 建议给云 WAF 的 ECS 单独绑定一个弹性 IP，若部署环境中存在 NAT 网关等，根据实际环境进行调整。</p>
10	安全组	<p>安全组类似防火墙功能，是一个逻辑上的分组，用于设置网络访问控制。您可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。</p> <p>安全组默认出方向放行，并且安全组内的云服务器可以相互访问。</p> <p>部署云 WAF 建议放通 TCP22（SSH 运维，使用完成后再删除放通规则）、TCP4431（Web 控制台）、TCP443（HTTPS 端口用于反向代理 HTTPS 网站）、TCP80 端口（HTTP 端口用于反向代理 HTTP 网站）、TCP20001（检测节点连接管理节点端口）、TCP6970（插件引流端口，若是多核 CPU 则需要放通的端口号从 6970 开始依次递增，一个检测节点有多少核 CPU，就可以配置多少个端口）及其他反向代理需要使用的端口；出方向放通云 WAF 到业务服务器的 IP 及端口。</p>
11	登录凭证	设置 ECS 服务器的后台账号密码。
12	实例名称	设置 ECS 服务器的名称。
13	实例描述	设置 ECS 服务器的描述，可留空。
14	高级选项	部署云 WAF 可以根据实际情况配置此功能，也可不配置。
15	资源标签	<p>基于标签您可以更灵活地管理成本分摊和财务分账；设置标签键自动创建云监控应用分组查看分组监控数据；对分组资源进行自动化运维管理。</p> <p>部署云 WAF 可以根据实际情况配置此功能，也可不配置。</p>

地域与计费

计费方式 按年计费 按月计费 按时计费 ^①
 按时计费会在每个月度根据您的使用情况向您提供账单，需要提前充值。

地域 ^②
 不同地域的实例之间内网互不相通；选择靠近您的地域，可降低网络时延，提高您的访问速度。
 移动云各资源池命名全新改版，若您对新旧资源池命名关系存在疑惑，可查看[资源池名称新旧映射表](#)

实例

架构

分类 通用型 通用网络优化型 内存优化型 内存网络优化型 超大内存型 计算型 计算网络优化型 超密主机型 大数据型 通用网络增强型

规格

规格族	规格名称	CPU型号/主频	vCPU(核)	内存(GB)	网络带宽能力(Gbit/s)	参考价格(元/小时)
<input type="radio"/>	通用型	s1.medium.2	Intel Xeon Gold 5118@2.3GHz	1	2	0.190元/小时
<input type="radio"/>	通用型	s1.medium.4	Intel Xeon Gold 5118@2.3GHz	1	4	0.320元/小时
<input type="radio"/>	通用型	s1.large.1	Intel Xeon Gold 5118@2.3GHz	2	2	0.350元/小时
<input checked="" type="radio"/>	通用型	s1.large.2	Intel Xeon Gold 5118@2.3GHz	2	4	0.390元/小时
<input type="radio"/>	通用型	s1.large.4	Intel Xeon Gold 5118@2.3GHz	2	8	0.500元/小时

当前选择实例

镜像

* 镜像来源 安全加固 ^③

存储

* 系统盘 GB

不同类型云硬盘性能指标不同，查看 [各类云硬盘性能指标](#)

启用自动备份 (推荐开启)
 利用云主机备份服务定期针对云盘进行备份，以应对病毒感染、数据误删等风险。 [了解更多](#)

数据盘 您已选择 0 块数据盘，还可以选择 5 块

[④添加数据盘](#)

*** 网络** 虚拟私有云

vpc_default subnet_default(2409:8c50:fff) 可用私有IP数量253个

如现有虚拟私有云/子网不符合您的要求，可以去控制台 [新建虚拟私有云](#) 或 [新建子网](#)

默认网卡 手动设置

公网IP 现在购买 暂不购买 使用已有

IPv4 IPv6 IPv4+IPv6

带宽计费方式 按固定带宽计费 按使用流量计费

接入类型 弹性公网IP

弹性公网IP默认关闭80、8080、443、8443端口，如需使用，请您先进行ICP备案，备案通过后为您开通上述端口！

*** 带宽** 0 Mbps

请手动调整带宽，默认0Mbps为不开通带宽，最大规格为500Mbps，如需订购更大带宽，请通过[工单申请](#)。

安全组 重新选择安全组

default x

首次申请会创建一个默认安全组 default，您也可以到控制台 [新建安全组](#)，[了解更多](#)。
为保障您云主机的安全性，请您修改云主机默认ssh端口及禁止root用户直接登录。[如何配置？](#) [了解更多](#)
如果您需要远程访问您的云主机，请确保在安全组开放特定端口（Linux需开放22端口，Windows需开放3389端口），[如何配置？](#) [其他问题？](#)

*** 登录凭证** 自定义密码 密钥对 创建后配置

*** 登录密码**

*** 确认密码**

请牢记您所设置的密码，如遗忘可登录ECS控制台重置密码，若不勾选 密钥对 / 自定义密码，则默认为创建后再设置
云主机安全组默认放通22端口和3389端口已实现公网访问，使用自定义密码会导致云主机被暴力破解，建议您使用密钥对创建实例。

*** 实例名称**

5~22位的英文、*、数字的组合，*不能在名称的开头和末尾。批量购买时自动加上三位数字的后缀
如：主机名为host；则命名为host-001、host-002，以此类推

实例描述

高级选项 云主机自定义数据

资源标签	标签键	标签值
+ 添加		

标签由区分大小写的键值对组成。例如，您可以添加一个键为"Group"且值为"Web"的标签。
标签键不可以重复，最长为127位；标签值不可以为空，最长为255位。标签键和标签值都不能以"ecloud"开头。
您最多可以设置10个标签，设置的标签将应用在本次创建的所有实例

3.1.2.6. 联通云

步骤1. 注册登录到联通云中，进入[产品/云基础产品/计算/云服务器ECS]中。



步骤2. 点击<立即购买>，跳转购买页面。

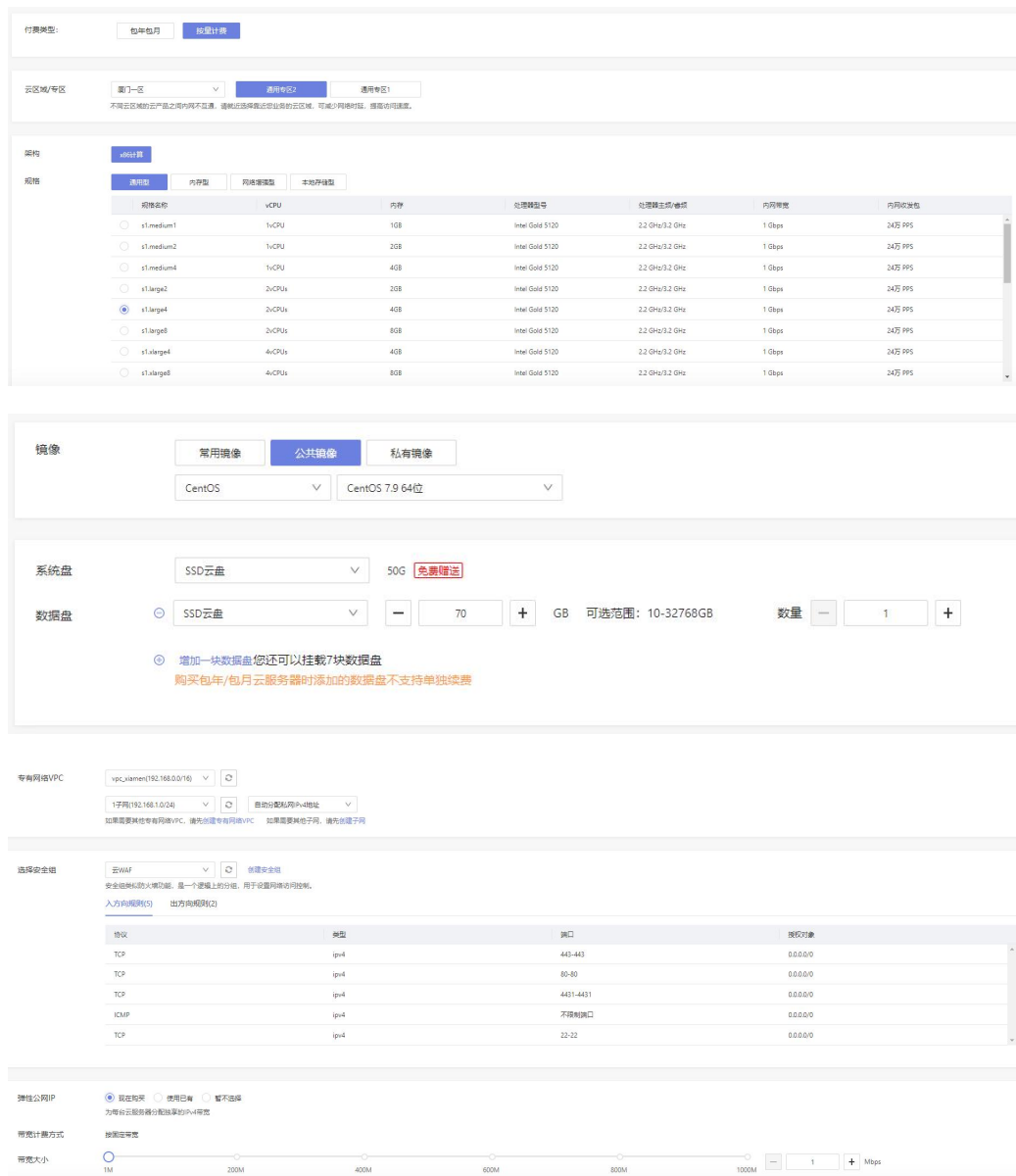


步骤3. 购买ECS服务器，配置购买服务器参数

序号	参数	说明
01	付费类型	<p>计费模式根据业务实际情况购买，例如在测试环境下，仅需部署两三天可以选择按需计费模式，在生产环境部署长期使用可以选择包年/包月模式。</p> <ul style="list-style-type: none"> ● 包年/包月 包年包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。 ● 按需计费 按需计费是后付费模式，按弹性云服务器的实际使用时长计费，可以随时开通/删除弹性云服务器。
02	云区域/专区	不同云区域的云产品之间内网不互通，请就近选择靠近您业务的云区域，可减少网络时延，提高访问速度。

03	架构	<p>部署云 WAF 选择 x86 计算架构。</p> <ul style="list-style-type: none"> ● x86 计算 <p>x86 CPU 架构采用复杂指令集（CISC），CISC 指令集的每个小指令可以执行一些较低阶的硬件操作，指令数目多而且复杂，每条指令的长度并不相同。由于指令执行较为复杂所以每条指令花费的时间较长。</p>
04	规格	<p>同一实例类型根据 CPU 和内存的配置不同分为多种实例规格，针对不同的应用场景，可以选择不同规格的弹性云服务器。</p> <p>云 WAF 的 CPU 内存选型可参考 2.2 章节，最低 2C4G。</p>
05	镜像	<p>镜像是一个包含了操作系统及必要配置的弹性云服务器模板，使用镜像可以创建弹性云服务器。</p> <p>部署云 WAF 选择公共镜像-Cent OS-Cent OS 7.9 64bit</p>
06	系统盘	<p>系统盘用于存储云服务器的操作系统，创建云服务器时自带系统盘，且系统盘自动初始化。</p> <p>部署云 WAF 建议磁盘盘 100G 以上，联通云默认系统盘 50G，则再添加一块数据盘 64G 及以上，系统启动后需挂载使用。</p>
07	网络	<p>虚拟私有云（VPC）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，可以在 VPC 中定义安全组、VPN、IP 地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。提升用户云上资源的安全性，简化用户的网络部署。</p> <p>不同虚拟私有云里面的弹性云服务器网络默认不通。</p>
08	安全组	<p>安全组类似防火墙功能，是一个逻辑上的分组，用于设置网络访问控制。您可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。</p> <p>安全组默认出方向放行，并且安全组内的云服务器可以相互访问。</p> <p>部署云 WAF 建议放通 TCP22（SSH 运维，使用完成后删除放通规则）、TCP4431（Web 控制台）、TCP443（HTTPS 端口用于反向代理 HTTPS 网站）、TCP80 端口（HTTP 端口用于反向代理 HTTP 网站）、TCP20001（检测节点连接管理节点端口）、TCP6970（插件引流端口，若是多核 CPU 则需要放通的端口号从 6970 开始依次递增，一个检测节点有多少核 CPU，就可以配置多少个端口）及其他反向代理需要使用的端口；出方向放通云 WAF 到业务服务器的 IP 及端口。</p>
09	弹性公网 IP	<p>弹性公网 IP 为云服务器提供访问外网的能力，可以灵活绑定及解绑，随时修改带宽。未绑定弹性公网 IP 的云服务器无法直接访问外网，无法直接对外进行互通信。</p> <p>一个弹性公网 IP 只能给一个 ECS 使用，不可以跨区域或跨账号使用，弹性公网 IP 和云服务器必须在同一个区域。</p> <p>部署云 WAF 建议给云 WAF 的 ECS 单独绑定一个弹性 IP，若部署环境中 NAT 网关等，根据实际环境进行调整。</p>
10	实例名称	设置 ECS 服务器的名称。
11	登录方式	设置 ECS 服务器的后台账号密码。
12	云服务器组	通过云服务器组功能，弹性云服务器在创建时，将尽量分

		<p>散地创建在不同的主机上，提高业务的可靠性。</p> <p>部署云 WAF 可以根据实际情况勾选或不勾选此功能。</p>
13	资源组	<p>在单个云账号下将一组相关资源进行统一管理的容器，一个资源只能归属于一个资源组。根据不同的业务场景，您可以将资源组映射为项目、应用或组织等概念。</p> <p>部署云 WAF 可以根据实际情况配置此功能，也可不配置。</p>
14	专属宿主机	<p>专属宿主机是联通云专为企业客户定制优化的解决方案，具有物理资源独享、部署更灵活、配置更丰富、性价比更高等特点，可以有效地降低企业上云的 TCO。</p> <p>部署云 WAF 可以根据实际情况配置此功能，也可不配置。</p>
15	购买数量	<p>根据实际需求选择购买云服务器器的数量。</p>



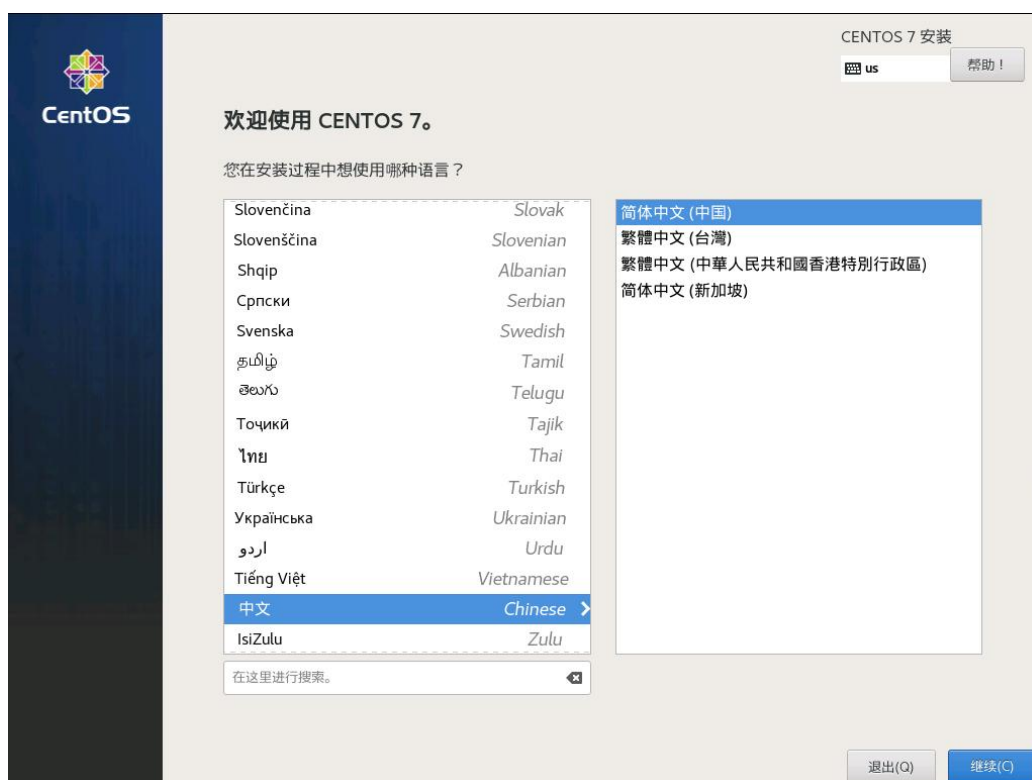
实例名称	<input type="text" value="云WAF"/>
登陆方式	<input checked="" type="radio"/> 密码 <input type="radio"/> 密钥对
登录名	root
登录密码	<input type="password" value="....."/>   <small>请妥善保管密码,如遗忘可在ECS控制台重置密码</small>
确认密码	<input type="password" value="....."/>  
云服务器组	<input type="checkbox"/> 开启反亲和性 
资源组	<input type="text" value="默认资源组"/>  
专属宿主机	<input type="text" value="请选择专属宿主机"/>   创建专属宿主机
购买数量	<input type="button" value="-"/> <input type="text" value="1"/> <input type="button" value="+"/> 台 <small>您最多可以创建 50 台云服务器</small>

3.2. 安装 CentOS 系统

步骤1. 加载完成后进入安装选项，选择<Install CentOS 7>。



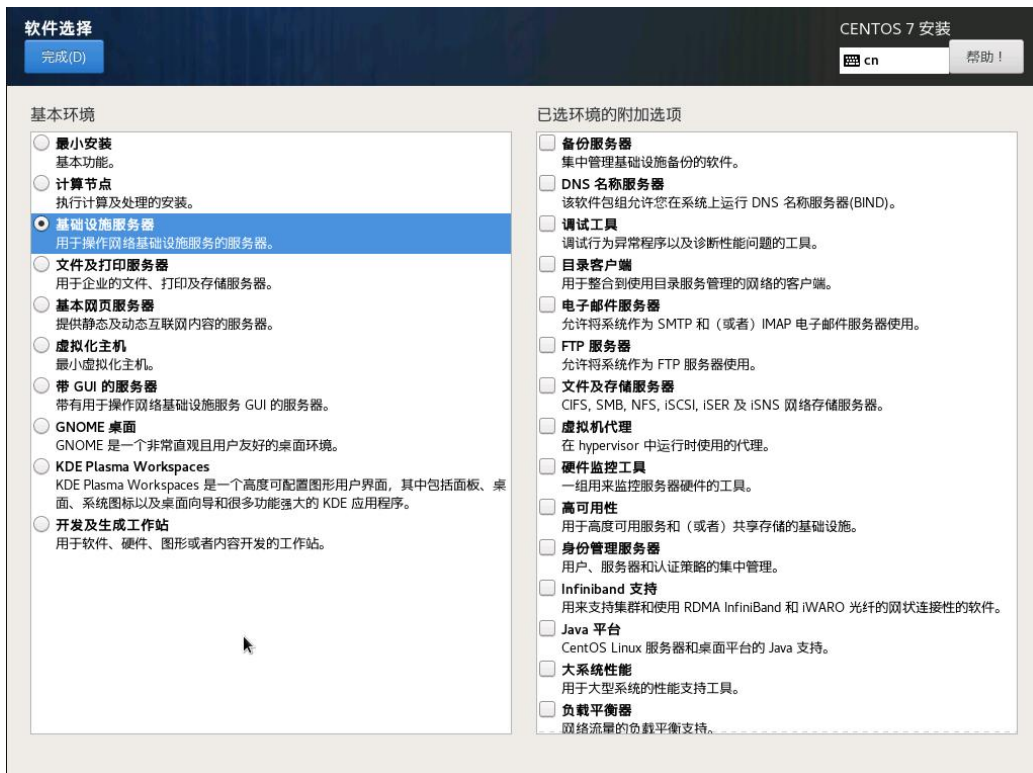
步骤2. 选择安装Cent OS 7的语言。



步骤3. 配置Cent OS 7的安装信息摘要。

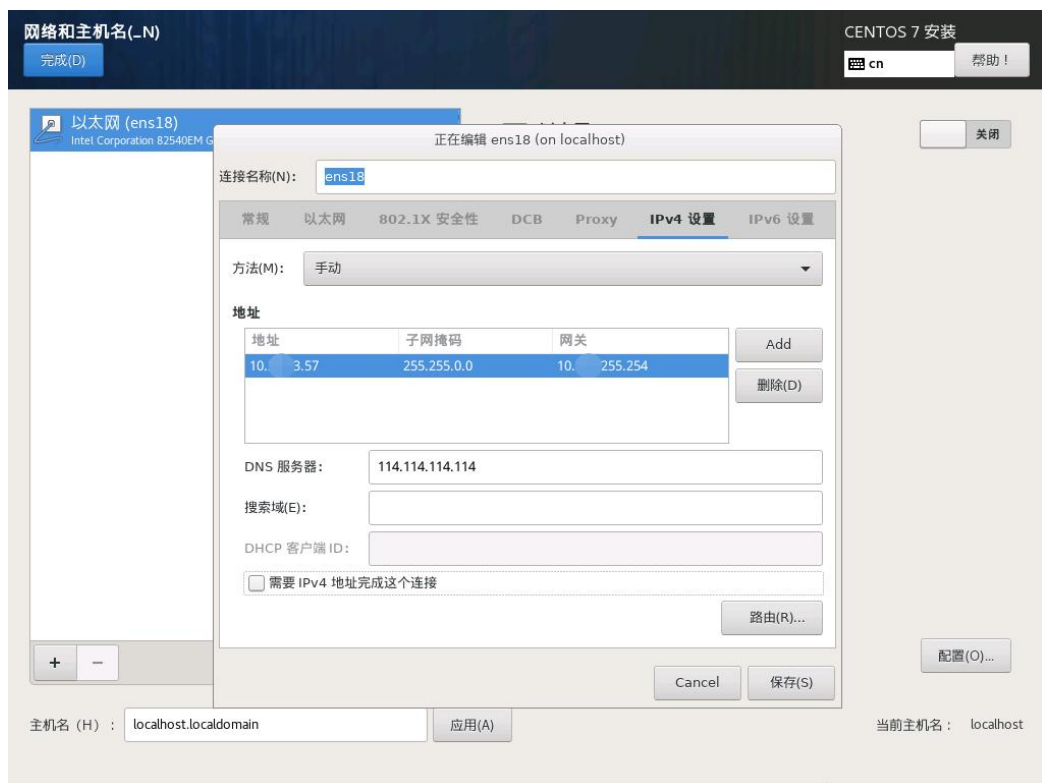
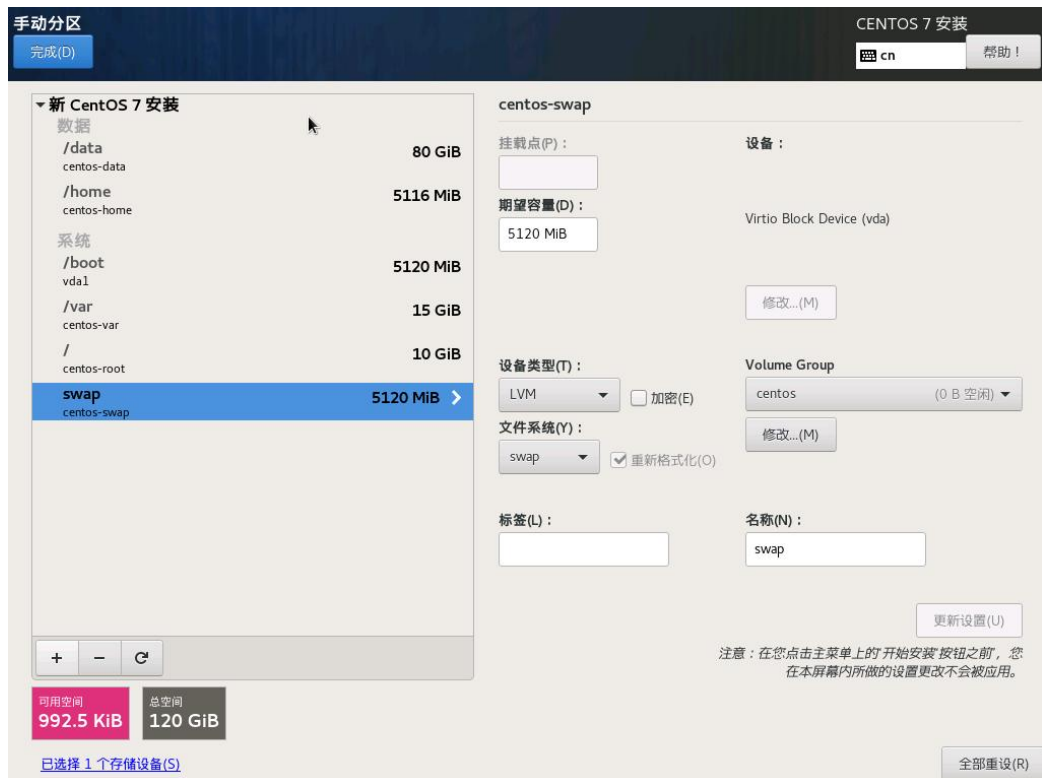


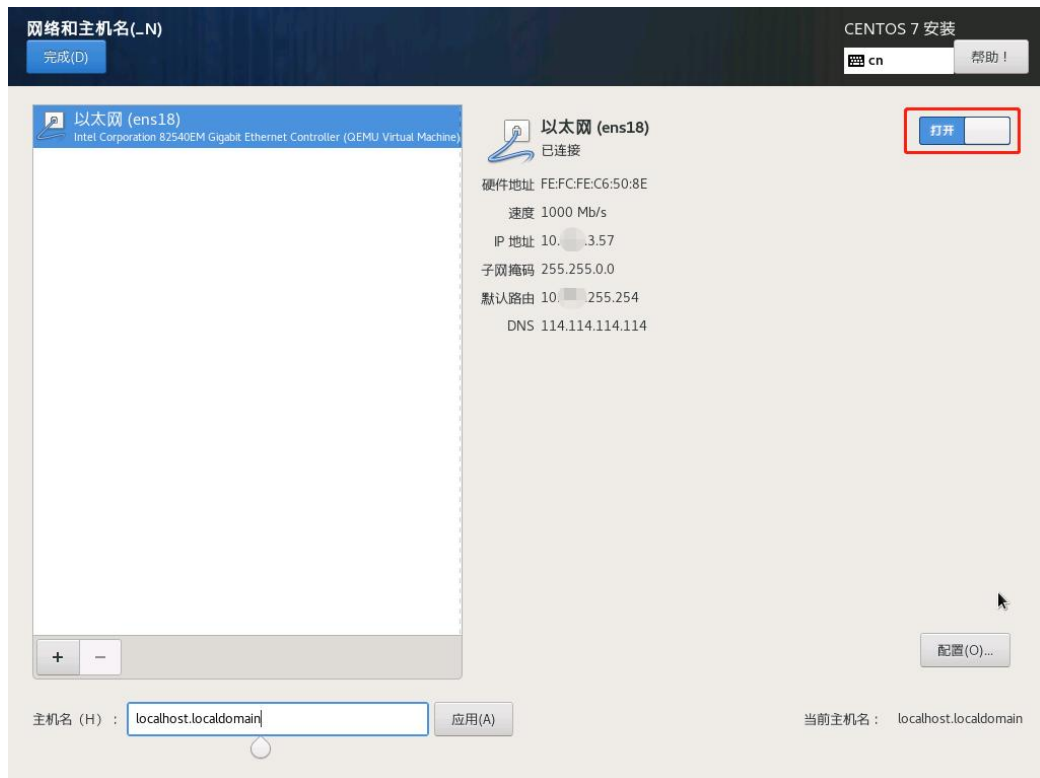
- 本地化：时间、键盘、语言等设置根据实际情况选择配置；
- 软件：安装源保持默认，软件选择中可以选择“基础设施服务器”的方式；



- 系统：安装位置不建议使用自动分配，手动配置分区，因为 WAF 的挂载目录要求大于 64G，推荐/var 分区 15G 以上，/分区 10G 以上，使用自动分区

可能无法达到此要求，本案例使用/data 分区安装云 WAF。配置好 IP 地址，其他选项保持默认即可。





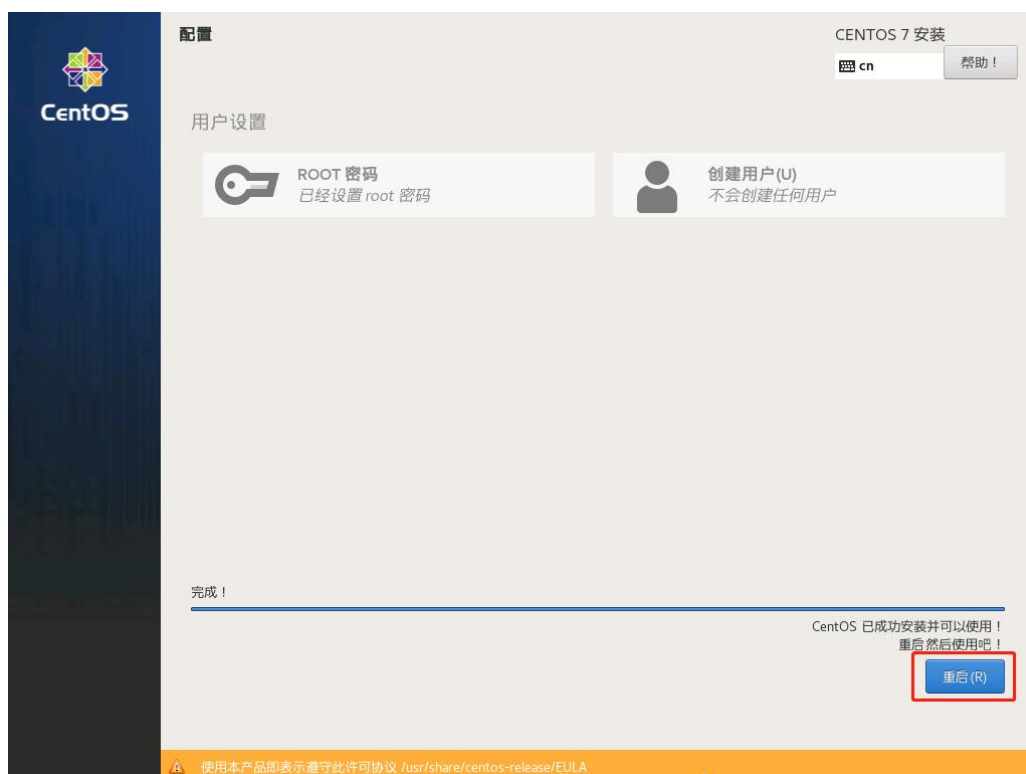
步骤4. 配置完所有参数后点击<开始安装>即可安装Cent OS 7系统。



步骤5. 在安装过程中，可以进行用户设置操作。



步骤6. 安装完成后重启系统即可完成安装。



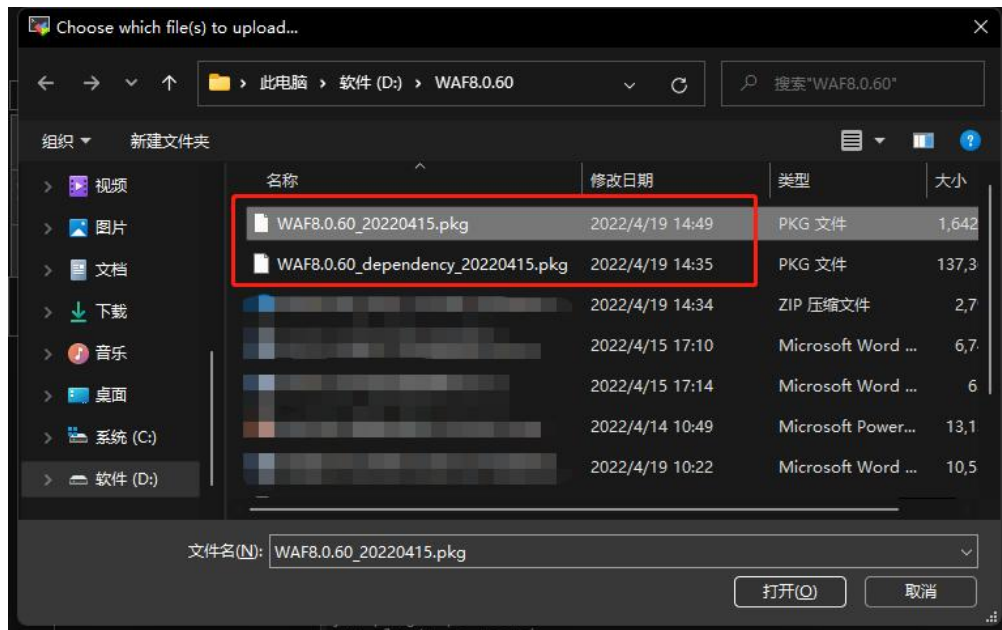
3.3. 安装云 WAF

云WAF安装包列表如下：

序号	文件名称	文件说明
01	WAF8.0.61_dependency_20220812.pkg	WAF 软件依赖安装包，包含安装 WAF 所依赖的 docker 软件，支持离线和在线两种安装模式。
02	WAF8.0.61_20220812.pkg	WAF8.0.61 软件安装包。
03	WAF8.0.61_plugin_module_20220812.zip	包含云 WAFso 引流插件和引流配置模板。

3.3.1. 单台设备反向代理模式

步骤1. 使用远程工具连接CentOS 7系统，并上传云WAF软件依赖安装包与安装包到/tmp目录下。



步骤2. 在宿主机中，关闭firewalld防火墙和SELinux服务。

- 关闭防火墙： `systemctl stop firewalld.service`
- 永久关闭防火墙： `systemctl disable firewalld.service`
- 关闭 SELinux： `setenforce 0`
- 永久关闭 SELinux： `vi /etc/selinux/config`，将 `SELINUX=enforcing` 改为 `SELINUX=disabled`，并重启设备。

```
[root@qianduoduo ~]# systemctl stop firewalld.service
[root@qianduoduo ~]# systemctl disable firewalld.service
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
```

```
[root@waf-fefcfe40384a tmp]# setenforce 0
setenforce: SELinux is disabled
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

步骤3. 给云WAF的依赖包执行权限。

chmod +x /tmp/[云WAF软件依赖安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_dependency_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 137368
drwx----- 3 root root    17 4月   8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJXSj
-rwxr-xr-x  1 root root 140664292 4月  19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤4. 安装云WAF的依赖包。


若设备能联网优先推荐使用在线安装，无网情况使用离线安装方式。

进入云WAF依赖包存放目录后执行安装命令。

cd /tmp

- 离线：./[云 WAF 软件依赖安装包名]
- 在线：./[云 WAF 软件依赖安装包名] -online

安装时输入 y 确认安装，输入 N 取消安装。

 注意：

WAF 依赖包安装时，会列表展示出要**卸载**和安装的宿主机程序，请确认后再进行下一步。

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_dependency_20220415.pkg -onl,net
Dependencies Resolved

Package arch Version Size
-----
Installing:
docker-ce x86_64 20.10.10-3.el7 23M

Package Summary
-----
Install 1 dependent packages
Is this ok [y/N]: y

Installing package docker:
已知数据源: fastestmirror, langpacks
正在检查 containerd.io-1.4.11-3-1.el7.x86_64.rpm: containerd.io-1.4.11-3-1.el7.x86_64.rpm, 不更新已安装的软件包。
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 3:docker-ce-20.10.10-3.el7.x86_64
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 安装失败
正在检查 docker-ce-cli-20.10.10-3.el7.x86_64.rpm: 3:docker-ce-cli-20.10.10-3.el7.x86_64
docker-ce-cli-20.10.10-3.el7.x86_64.rpm: 不更新已安装的软件包。
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: docker-ce-rootless-extras-20.10.10-3.el7.x86_64
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: 安装失败
正在检查 docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: docker-scan-plugin-0.9.0-3.el7.x86_64
docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: 不更新已安装的软件包。
正在检查软件包:
--> 正在检查事务
--> 软件包 docker-ce.x86_64.2.20.10.10-3.el7 将被 安装
--> 软件包 docker-ce-rootless-extras.x86_64.0.20.10.10-3.el7 将被 安装
--> 解决依赖关系完成

依赖关系解决

Package 架构 版本 源 大小
-----
正在安装:
docker-ce x86_64 3:20.10.10-3.el7 /docker-ce-20.10.10-3.el7.x86_64 96 M
docker-ce-rootless-extras x86_64 20.10.10-3.el7 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64 20 M

事务概要
-----
安装 2 软件包
总计, 116 M
安装大小: 116 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
正在安装 : 3:docker-ce-20.10.10-3.el7.x86_64 1/2
正在安装 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 2/2
验证中 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 1/2
验证中 : 3:docker-ce-20.10.10-3.el7.x86_64 2/2
```

步骤5. 安装完成后，执行docker ps查看docker是否运行

```
[root@waf-fefcfe40384a tmp]# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
[root@waf-fefcfe40384a tmp]# docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
[root@waf-fefcfe40384a tmp]# ps -aux | grep docker
root 8023 0.0 1.5 1163304 60152 ? Ssl 15:44 0:00 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root 21231 0.0 0.0 112728 972 pts/0 R+ 16:16 0:00 grep --color=auto docker
[root@waf-fefcfe40384a tmp]#
```

步骤6. 安装云WAF安装包，给云WAF安装包执行权限。

chmod +x /tmp/[云WAF安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 1779488
drwxr-xr-x 3 root root 17 4月 8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-DUJXSj
-rwxr-xr-x 1 root root 1681526916 4月 19 16:10 WAF8.0.60_20220415.pkg
-rwxr-xr-x 1 root root 140664292 4月 19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤7. 安装云WAF的安装包，并输入挂载路径和密码

8O#NII@QXIZrW^c&%KPqIc#Y并选择部署角色为Management Platform + WAF Agent（管理节点+检测节点），回车确认。

cd /tmp

./[云WAF安装包名]

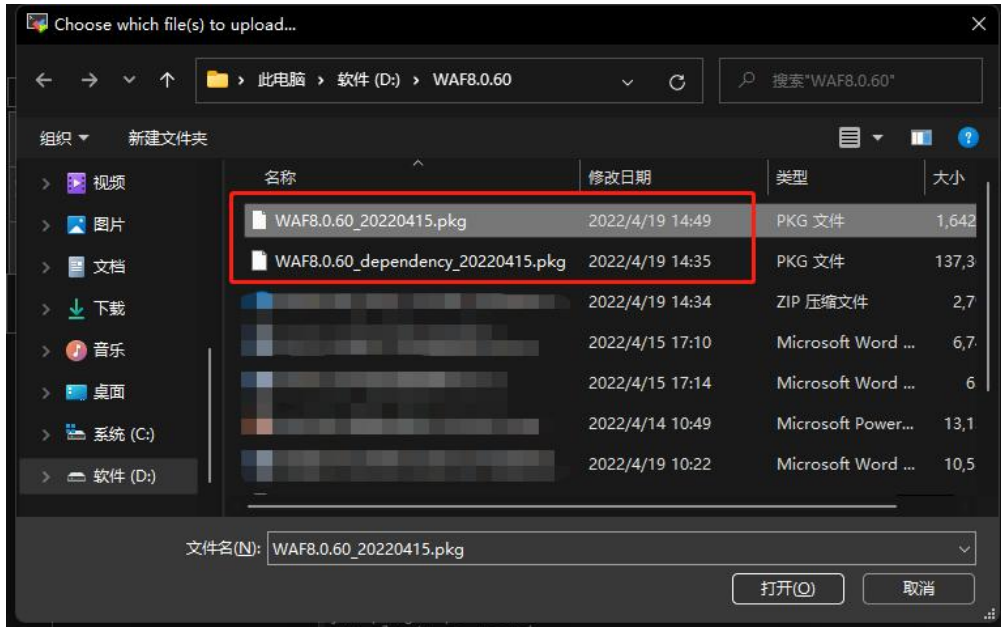
注意：安装路径并非一定为/data，可自定义创建文件目录，空间满足大于64G即可

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_20220415.pkg
Please enter the mount path: /data
x Please enter the password: *****
Use the arrow keys to navigate: ↑ ↓ → ← and / toggles search
Select Deployment Role
* Management Platform + WAF Agent
  Management Platform
  WAF Agent
----- Selected Deployment Role -----
Management Platform + WAF Agent
```

步骤8. 选择需要部署模式为Reverse Proxy（反向代理），回车确认。

3.3.2. 单台设备插件模式

步骤1. 使用远程工具连接Cent OS 7系统，并上传云WAF软件依赖安装包与安装包到/tmp目录下。



步骤2. 在宿主机中，关闭firewalld防火墙和SELinux服务。

- 关闭防火墙：systemctl stop firewalld.service
- 永久关闭防火墙：systemctl disable firewalld.service
- 关闭 SELinux：setenforce 0
- 永久关闭 SELinux：vi /etc/selinux/config，将 SELINUX=enforcing 改为 SELINUX=disabled，并重启设备。

```
[root@qianduoduo ~]# systemctl stop firewalld.service
[root@qianduoduo ~]# systemctl disable firewalld.service
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
```

```
[root@waf-fefcfe40384a tmp]# setenforce 0
setenforce: SELinux is disabled
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

步骤3. 给云WAF的依赖包执行权限。

chmod +x /tmp/[云WAF软件依赖安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_dependency_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 137368
drwx----- 3 root root      17 4月   8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJXSj
-rwxr-xr-x  1 root root 140664292 4月   19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤4. 安装云WAF的依赖包。

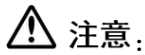
若设备能联网优先推荐使用在线安装，无网情况使用离线安装方式。

进入云WAF依赖包存放目录后执行安装命令。

cd /tmp

- 离线：./[云 WAF 软件依赖安装包名]
- 在线：./[云 WAF 软件依赖安装包名] -online

安装时输入 y 确认安装，输入 N 取消安装。



注意：

WAF 依赖包安装时，会列表展示出要卸载和安装的宿主机程序，请确认后再进行下一步。

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_dependency_20220415.pkg -online
Dependencies Resolved

Package Arch Version Size
Installing:
docker-ce x86_64 20.10.10-3.el7 23M
Package Summary
-----
Install 1 dependent packages
Is this ok [Y/N]: y

Installing package docker:
已加载插件：fastestmirror, langpacks
正在检查 containerd.io-1.4.11-3.el7.x86_64.rpm: containerd.io-1.4.11-3.el7.x86_64
containerd.io-1.4.11-3.el7.x86_64.rpm，不更新已安装的软件包。
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 3:docker-ce-20.10.10-3.el7.x86_64
docker-ce-20.10.10-3.el7.x86_64.rpm 将被安装。
正在检查 docker-ce-cli-20.10.10-3.el7.x86_64.rpm: 1:docker-ce-cli-20.10.10-3.el7.x86_64
docker-ce-cli-20.10.10-3.el7.x86_64.rpm，不更新已安装的软件包。
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: docker-ce-rootless-extras-20.10.10-3.el7.x86_64
docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm 将被安装。
正在检查 docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: docker-scan-plugin-0.9.0-3.el7.x86_64
docker-scan-plugin-0.9.0-3.el7.x86_64.rpm，不更新已安装的软件包。
正在解决依赖关系
--> 正在检查事务
--> 软件包 docker-ce.x86_64.3.20.10.10-3.el7 将被 安装
--> 软件包 docker-ce-rootless-extras.x86_64.0.20.10.10-3.el7 将被 安装
--> 解决依赖关系完成

依赖关系解决

Package 架构 版本 源 大小
-----
正在安装:
docker-ce x86_64 3:20.10.10-3.el7 /docker-ce-20.10.10-3.el7.x86_64 96 M
docker-ce-rootless-extras x86_64 20.10.10-3.el7 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64 20 M
事务概要
-----
安装 2 软件包
总计：116 M
安装大小：116 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing : 3:docker-ce-20.10.10-3.el7.x86_64 1/2
正在安装 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 2/2
验证中 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 1/2
验证中 : 3:docker-ce-20.10.10-3.el7.x86_64 2/2
```

步骤5. 安装完成后，执行docker ps查看docker是否运行

```
[root@waf-fefcfe40384a tmp]# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
[root@waf-fefcfe40384a tmp]# docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
[root@waf-fefcfe40384a tmp]# ps -aux | grep docker
root 8023 0.0 1.5 1163304 60152 ? Ssl 15:44 0:00 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root 21231 0.0 0.0 112728 972 pts/0 R+ 16:16 0:00 grep --color=auto docker
[root@waf-fefcfe40384a tmp]#
```

步骤6. 安装云WAF安装包，给云WAF安装包执行权限。

chmod +x /tmp/[云WAF安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 1779408
drwx----- 3 root root      17 4月   8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJXSj
-rwxr-xr-x  1 root root 1681526916 4月   19 16:10 WAF8.0.60_20220415.pkg
-rwxr-xr-x  1 root root 140664292 4月   19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤7. 安装云WAF的安装包，并输入挂载路径和密码

8O#NII@QXIZrW^c&%KPqlc#Y并选择部署角色为Management Platform + WAF Agent（管理节点+检测节点），回车确认。

/cd/tmp

./[云WAF安装包名]

注意：安装路径并非一定为/data，可自定义创建文件目录，空间满足大于64G即可

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_20220415.pkg
Please enter the mount path: /data
* Please enter the password: *****
Use the arrow keys to navigate: ↑ ↓ → ← and / toggles search
Select Deployment Role
  * Management Platform + WAF Agent
    Management Platform
    WAF Agent

----- Selected Deployment Role -----
Management Platform + WAF Agent
```

步骤8. 选择需要部署模式为（插件），回车确认。

```
Write out database with 1 new entries
Data Base Updated
Use the arrow keys to navigate: ↑ ↓ → ← and / toggles search
Select Deployment Method
  Reverse Proxy
  * Plugin

----- Selected Deployment Method -----
Plugin
```

```
Certificate is to be certified until Apr 12 11:05:42 2052 GMT (10950 days)

Write out database with 1 new entries
Data Base Updated
Deployment Method: Plugin
2653d992f4ef: Loading layer [=====] 216.5MB/216.5MB
f1affad69343: Loading layer [=====] 181.4MB/181.4MB
18a6d2a77388: Loading layer [=====] 150kB/150kB
c377c28a3e43: Loading layer [=====] 52.85MB/52.85MB
914120db83a9: Loading layer [=====] 1.077GB/1.077GB
8d1dc0b00b3f: Loading layer [=====] 13.82kB/13.82kB
360f6aa95169: Loading layer [=====] 2.264MB/2.264MB
a93f4df02f78: Loading layer [=====] 434.2kB/434.2kB
17fc118b9866: Loading layer [=====] 5.632kB/5.632kB
e311caf2fa28: Loading layer [=====] 4.096kB/4.096kB
ab2eb94ebe5e: Loading layer [=====] 440.3MB/440.3MB
d1d23d2c1f83: Loading layer [=====] 5.12kB/5.12kB
62b40fdf1aa3: Loading layer [=====] 2.189MB/2.189MB
0268ba6f0efd: Loading layer [=====] 4.096kB/4.096kB
Loaded image: waf_detect:8.0.60.321B
```

步骤9. 安装成功后，使用以下命令检查安装是否正常。安装成功后，云WAF会有waf_mgt、waf_redis、waf_detect三个容器正在运行。

列出所有在运行的容器信息：doker ps

列出本地镜像：docker images

```
[root@waf-fefcfe2b045 tmp]# docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS
21d148fde895  waf_detect:8.0.60.321B             "/bin/sh -c 'chmod +..." 22 minutes ago Up 21 minutes 0.0.0.0:6970-6971->6970-6971/tcp, :::6970-6971->6970-6971/tcp
3b6c96e81eap  waf_redis:latest                  "/opt/bitnami/script..." 22 minutes ago Up 21 minutes 6379/tcp, 127.0.0.1:6381->6381/tcp
cf46f19289d   waf_mgt:8.0.60.321B                "/bin/sh -c 'chmod +..." 22 minutes ago Up 21 minutes 0.0.0.0:4431->4431/tcp, :::4431->4431/tcp, 0.0.0.0:20901->20901/tcp, :::20901->20901/tcp
[root@waf-fefcfe2b045 tmp]# docker images
REPOSITORY    TAG      IMAGE ID       CREATED        SIZE
waf_detect    8.0.60.321B  0481b24da639  4 days ago    1.93GB
waf_redis     latest    3b6c36233b3   4 days ago    96.1MB
waf_mgt       8.0.60.321B  7057c095244   4 days ago    3.36GB
[root@waf-fefcfe2b045 tmp]#
```

步骤10. 将对应版本的so插件和引流配置模板拷贝到nginx安装目录，修改

nginx.conf的配置，将云WAF插件和引流配置模板配置进去，在include云WAF的配置模板时，需放到nginx.conf文件最后面。

```
root@5a7b541159f4:/# cat /etc/nginx/nginx.conf
user nginx;
worker_processes auto;

error_log /var/log/nginx/error.log notice;
pid /var/run/nginx.pid;
load_module /etc/nginx/nginx_1.21.6_http_waf_agent_module.so;

events {
    worker_connections 1024;
}

http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    sendfile on;
    #tcp_nopush on;

    keepalive_timeout 65;

    #gzip on;

    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/template.conf;
}
root@5a7b541159f4:/#
```

步骤11. 根据实际云WAF部署情况，修改template.conf引流配置文件。server配置表示把经过此nginx的流量引流到云WAF检测节点进行业务防护，填写的server IP为云WAF检测节点的IP，端口默认从6970开始依次递增，一个检测节点有多少核CPU，就可以配置多少个端口，如下图为2核的检测节点。

```
root@5a7b541159f4:/# cat /etc/nginx/template.conf
upstream waf_server {
    hash $remote_addr$remote_port;
    keepalive 512;

    #custom by cpu nums
    server 10.243.3.88:6970;
    server 10.243.3.88:6971;
}

waf_agent /waf_detect;
waf_agent_request_body_max_size 1m;
waf_filter /waf_detect;
waf_filter_buffer 1m;
waf_filter_reply_body_max_size 1m;

server_include {
    location /waf_detect {
        internal;
        waf_pass waf_server;
        waf_pass_connect_timeout 1s;
        waf_pass_read_timeout 1s;
        waf_pass_send_timeout 1s;
    }
}
root@5a7b541159f4:/#
```

⚠ 注意:

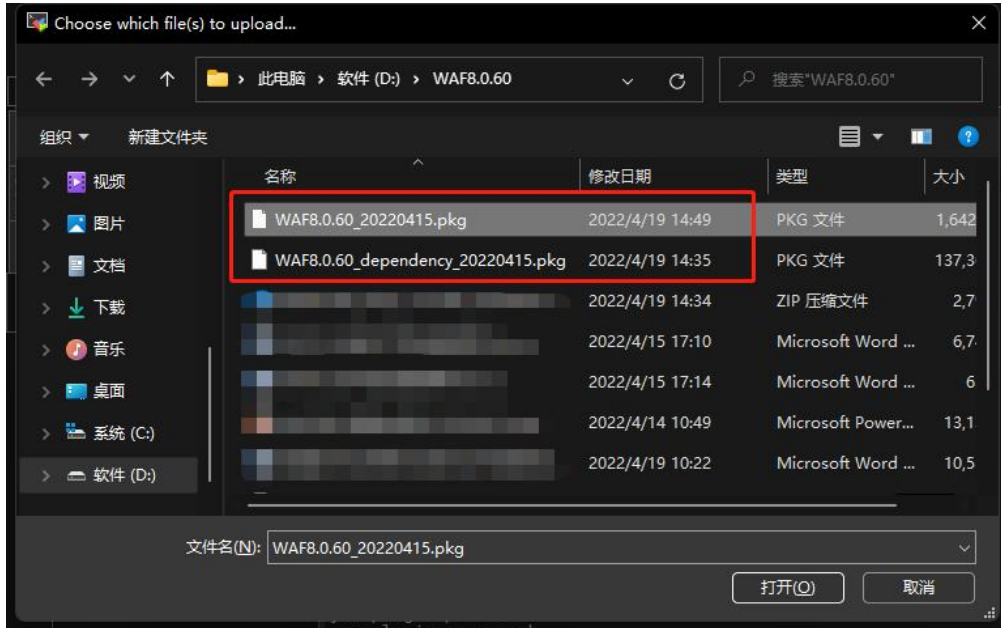
一个 nginx 可以配置多个检测节点的 IP。例如部署了 2 个 WAF 检测节点，一台检测节点有 2 核 CPU，一台检测节点有 4 核 CPU，则配置如下：

```
#custom by cpu nums
server 10.246.84.125:6970;
server 10.246.84.125:6971;
server 10.246.84.126:6970;
server 10.246.84.126:6971;
server 10.246.84.126:6972;
server 10.246.84.126:6973;
```

步骤12. 配置完插件后，重新启动nginx服务，让引流插件才能生效。

3.3.3. 分离式设备反向代理模式

步骤1. 在宿主机A上，使用远程工具连接Cent OS 7系统，并上传云WAF软件依赖安装包与安装包到/tmp目录下。



步骤2. 在宿主机A中，关闭firewalld防火墙和SELinux服务。

- 关闭防火墙：systemctl stop firewalld.service
- 永久关闭防火墙：systemctl disable firewalld.service
- 关闭 SELinux：setenforce 0
- 永久关闭 SELinux：vi /etc/selinux/config，将 SELINUX=enforcing 改为 SELINUX=disabled，并重启设备。

```
[root@qianduoduo ~]# systemctl stop firewalld.service
[root@qianduoduo ~]# systemctl disable firewalld.service
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
```

```
[root@waf-fefcfe40384a tmp]# setenforce 0
setenforce: SELinux is disabled
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

步骤3. 给云WAF的依赖包执行权限。

chmod +x /tmp/[云WAF软件依赖安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_dependency_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 137368
drwxr-xr-x 3 root root      17 4月  8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJXsj
-rwxr-xr-x 1 root root 140664292 4月 19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤4. 安装云WAF的依赖包。

若设备能联网优先推荐使用在线安装，无网情况使用离线安装方式。

进入云WAF依赖包存放目录后执行安装命令。

cd /tmp

- 离线：./[云 WAF 软件依赖安装包名]
- 在线：./[云 WAF 软件依赖安装包名] -online

安装时输入 y 确认安装，输入 N 取消安装。

⚠ 注意：

WAF 依赖包安装时，会列表展示出要卸载和安装的宿主主机程序，请确认后再进行下一步。

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_dependency_20220415.pkg -online
Dependencies Resolved

=====
Package Arch Version Size
=====
Installing:
docker-ce x86_64 20.10.10-3.el7 23M
Package Summary
=====
Install 1 dependent packages
Is this ok [Y/n]: y

Install package docker:
正在检查 fastestairroot langpacks
正在检查 containerd.io-1.4.11-3-1.el7.x86_64.rpm: containerd.io-1.4.11-3-1.el7.x86_64
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 3:docker-ce-20.10.10-3.el7.x86_64
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 将按安装
正在检查 docker-ce-cli-20.10.10-3.el7.x86_64.rpm: 1:docker-ce-cli-20.10.10-3.el7.x86_64
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: 不更新已安装的软件包
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: 将按安装
正在检查 docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: docker-scan-plugin-0.9.0-3.el7.x86_64
正在检查 docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: 不更新已安装的软件包
正在解决依赖关系
--> 软件包 docker-ce.x86_64.3.20.10.10-3.el7 将按 安装
--> 软件包 docker-ce-rootless-extras.x86_64.20.10.10-3.el7 将按 安装
--> 解决依赖关系完成

依赖关系解决

=====
Package 架构 版本 源 大小
=====
正在安装:
docker-ce x86_64 3:20.10.10-3.el7 /docker-ce-20.10.10-3.el7.x86_64 96 M
docker-ce-rootless-extras x86_64 20.10.10-3.el7 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64 20 M
事务概要

安装 2 软件包
总计 116 M
安装大小 116 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
正在安装 : 3:docker-ce-20.10.10-3.el7.x86_64 1/2
正在安装 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 2/2
验证中 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 1/2
验证中 : 3:docker-ce-20.10.10-3.el7.x86_64 2/2
```

步骤5. 安装完成后，执行docker ps查看docker是否运行

```
[root@waf-fefcfe40384a tmp]# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
[root@waf-fefcfe40384a tmp]# docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
[root@waf-fefcfe40384a tmp]# ps -aux | grep docker
root 8023 0.0 1.5 1163304 60152 ? Ssl 15:44 0:00 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root 21231 0.0 0.0 112728 972 pts/0 R+ 16:16 0:00 grep --color=auto docker
[root@waf-fefcfe40384a tmp]#
```

步骤6. 安装云WAF安装包，给云WAF安装包执行权限。

chmod +x /tmp/[云WAF安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 1779488
drwx----- 3 root root 17 4月 8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronydw.service-dujxsj
-rwxr-xr-x 1 root root 1681526916 4月 19 16:10 WAF8.0.60_20220415.pkg
-rwxr-xr-x 1 root root 140664292 4月 19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤7. 安装云WAF的安装包，并输入挂载路径和密码

8O#NII@QXIZrW^c&%KPqIc#Y并选择部署角色为Management Platform（管理节点），回车确认。

cd /tmp

./[云WAF安装包名]

注意：安装路径并非一定为/data，可自定义创建文件目录，空间满足大于64G即可

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_20220415.pkg
Please enter the mount path: /data
Please enter the password: *****
Use the arrow keys to navigate: ↓ ↑ → ← and / toggles search
Select Deployment Role
  Management Platform + WAF Agent
  * Management Platform
  WAF Agent

----- Selected Deployment Role -----
Management Platform
```

步骤8. 选择需要部署模式为Reverse Proxy（反向代理），回车确认。

```
X509v3 Basic Constraints:
  CA:FALSE
Netscape Comment:
  OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
  09:51:39:55:96:85:05:95:16:60:83:CE:5D:02:16:6A:01:36:C1:EE
X509v3 Authority Key Identifier:
  keyid:95:12:38:33:58:E7:5C:11:B0:33:52:4D:5E:B9:D5:84:4E:5B:D8:46

Certificate is to be certified until Apr 11 16:20:34 2052 GMT (10950 days)

Write out database with 1 new entries
Data Base Updated
Use the arrow keys to navigate: ↓ ↑ → ← and / toggles search
Select Deployment Method
  * Reverse Proxy
  Plugin

----- Selected Deployment Method -----
Reverse Proxy
```

```
Write out database with 1 new entries
Data Base Updated
Deployment Method: Reverse Proxy
2653d992f4ef: Loading layer [=====] 216.5MB/216.5MB
f1affad69343: Loading layer [=====] 181.4MB/181.4MB
18a6d2a77388: Loading layer [=====] 150kB/150kB
c377c28a3e43: Loading layer [=====] 52.85MB/52.85MB
914120db83a9: Loading layer [=====] 1.077GB/1.077GB
8d1dc0b00b3f: Loading layer [=====] 13.82kB/13.82kB
360f6aa95169: Loading layer [=====] 2.264MB/2.264MB
a93f4df02f78: Loading layer [=====] 434.2kB/434.2kB
17fc118b9866: Loading layer [=====] 5.632kB/5.632kB
e311caf2fa28: Loading layer [=====] 4.096kB/4.096kB
ab2eb94ebe5e: Loading layer [=====] 327MB/440.3MB
```

步骤9. 安装成功后，使用以下命令检查安装是否正常，安装成功后，云WAF管理节点会有waf_mgt和waf_redis两个容器正在运行。

列出所有在运行的容器信息：doker ps

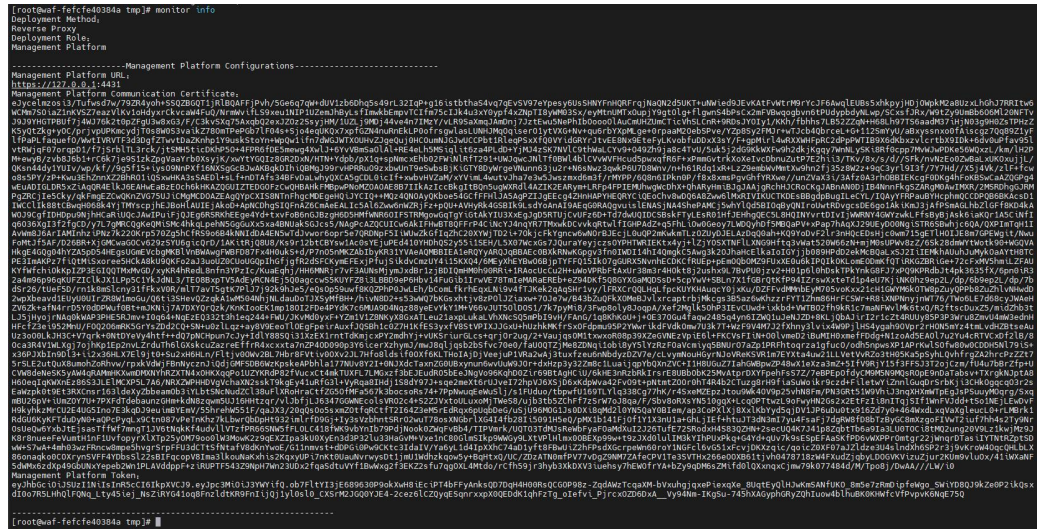
列出本地镜像：docker images

```
[root@waf-fefcfe40384a tmp]# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED    STATUS    PORTS
09c5b33f897   waf_mgt:8.0.60.321b   "/bin/sh -c 'chmod +..."   4 minutes ago   Up 4 minutes   0.0.0.0:4431->4431/tcp, :::4431->4431/tcp, 0.0.0.0:20801->20801/tcp, :::20801->20801/tcp
e546ad2958bc   waf_redis:latest    "/opt/bitnami/script..."   4 minutes ago   Up 4 minutes   6379/tcp, 127.0.0.1:6381->6381/tcp

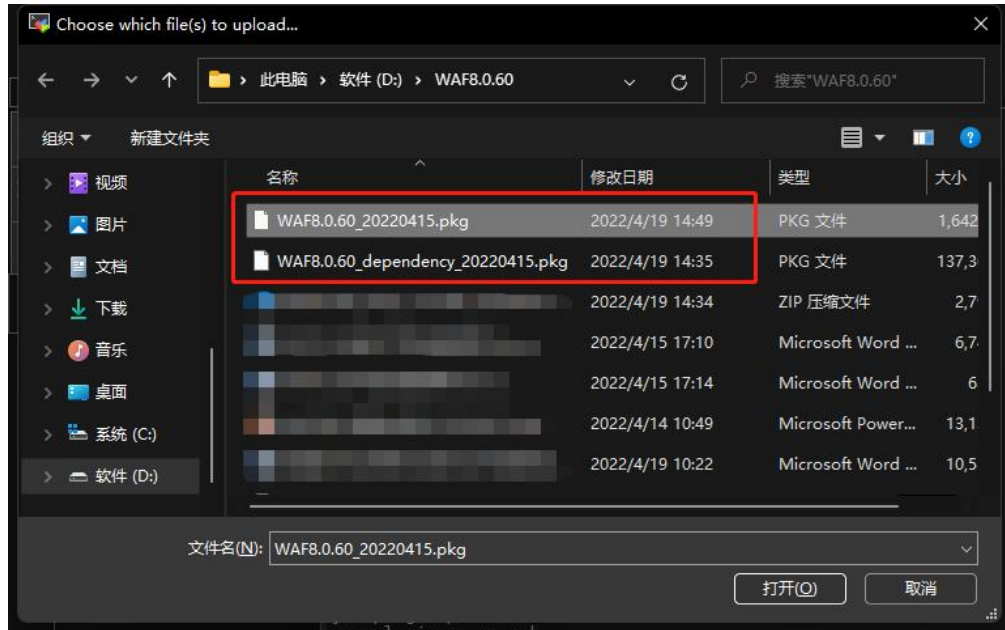
[root@waf-fefcfe40384a tmp]# docker images
REPOSITORY    TAG      IMAGE ID       CREATED    SIZE
waf_nginx     8.0.60.321b   e17be8cd3fa0   4 days ago   1.86B
waf_detect   8.0.60.321b   9481b24de39   4 days ago   1.93B
waf_redis    latest      3d86336238b3   4 days ago   96.1MB
waf_mgt      8.0.60.321b   7057cd99524d   4 days ago   3.38B
```

步骤10. 在宿主机A上执行以下命令获取管理节点的证书和Token信息，作为检测节点连接管理节点的凭证。

monitor info

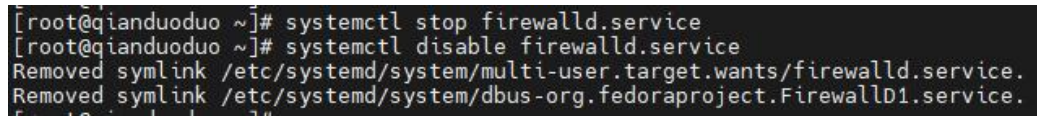


步骤11. 在宿主机B上，使用远程工具连接Cent OS 7系统，并上传WAF软件依赖安装包与安装包到/tmp目录下。



步骤12. 在宿主机B中，关闭firewalld防火墙和SELinux服务。

- 关闭防火墙: systemctl stop firewalld.service
- 永久关闭防火墙: systemctl disable firewalld.service
- 关闭 SELinux: setenforce 0
- 永久关闭 SELinux: vi /etc/selinux/config, 将 SELINUX=enforcing 改为 SELINUX=disabled, 并重启设备。



```
[root@waf-febfcfe40384a tmp]# setenforce 0
setenforce: SELinux is disabled
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

步骤13. 给云WAF的依赖包执行权限。

chmod +x /tmp/[云WAF软件依赖安装包名]

```
[root@waf-febfcfe40384a tmp]# chmod +x WAF8.0.60_dependency_20220415.pkg
[root@waf-febfcfe40384a tmp]# ll
总用量 137368
drwx----- 3 root root      17 4月  8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJX5j
-rwxr-xr-x 1 root root 140664292 4月 19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤14. 安装云WAF的依赖包。

若设备能联网优先推荐使用在线安装，无网情况使用离线安装方式。

进入云WAF依赖包存放目录后执行安装命令。

cd /tmp

- 离线：./[云 WAF 软件依赖安装包名]
- 在线：./[云 WAF 软件依赖安装包名] -online

安装时输入 y 确认安装，输入 N 取消安装。

⚠ 注意:

WAF 依赖包安装时，会列表展示出要卸载和安装的宿主主机程序，请确认后再进行下一步。

```
[root@waf-febfcfe40384a tmp]# ./WAF8.0.60_dependency_20220415.pkg -online
Dependencies Resolved

Package Arch Version Size
-----
Installing:
docker-ce x86_64 20.10.10-3.el7 23M

Package Summary
=====
Install 1 Dependent packages
(is this ok [y/N]?)
Installing package docker-
已加载插件：fastestmirror、langpacks
正在检查 containerd.io-1.4.11-3-1.el7.x86_64.rpm: containerd.io-1.4.11-3-1.el7.x86_64
containerd.io-1.4.11-3-1.el7.x86_64.rpm: 不更新已安装的软件包。
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 3:docker-ce-20.10.10-3.el7.x86_64
docker-ce-20.10.10-3.el7.x86_64.rpm 将被安装
正在检查 docker-ce-cli-20.10.10-3.el7.x86_64.rpm: 1:docker-ce-cli-20.10.10-3.el7.x86_64
docker-ce-cli-20.10.10-3.el7.x86_64.rpm: 不更新已安装的软件包。
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: docker-ce-rootless-extras-20.10.10-3.el7.x86_64
docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm 将被安装
正在检查 docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: docker-scan-plugin-0.9.0-3.el7.x86_64
docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: 不更新已安装的软件包。
正在解决依赖关系
--> 正在检查事务
--> 软件包 docker-ce.x86_64.3.20.10-3.el7 将被 安装
--> 软件包 docker-ce-rootless-extras.x86_64.20.10-3.el7 将被 安装
--> 解决依赖关系完成

依赖关系解决

Package 架构 版本 源 大小
-----
正在安装:
docker-ce0 x86_64 3:20.10.10-3.el7 /docker-ce-20.10.10-3.el7.x86_64 96 M
docker-ce-rootless-extras x86_64 20.10.10-3.el7 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64 20 M
事务概要
-----
安装 2 软件包
总计：116 M
安装大小：116 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
正在安装 : 3:docker-ce-20.10.10-3.el7.x86_64 1/2
正在安装 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 2/2
验证中 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 1/2
验证中 : 3:docker-ce-20.10.10-3.el7.x86_64 2/2
```

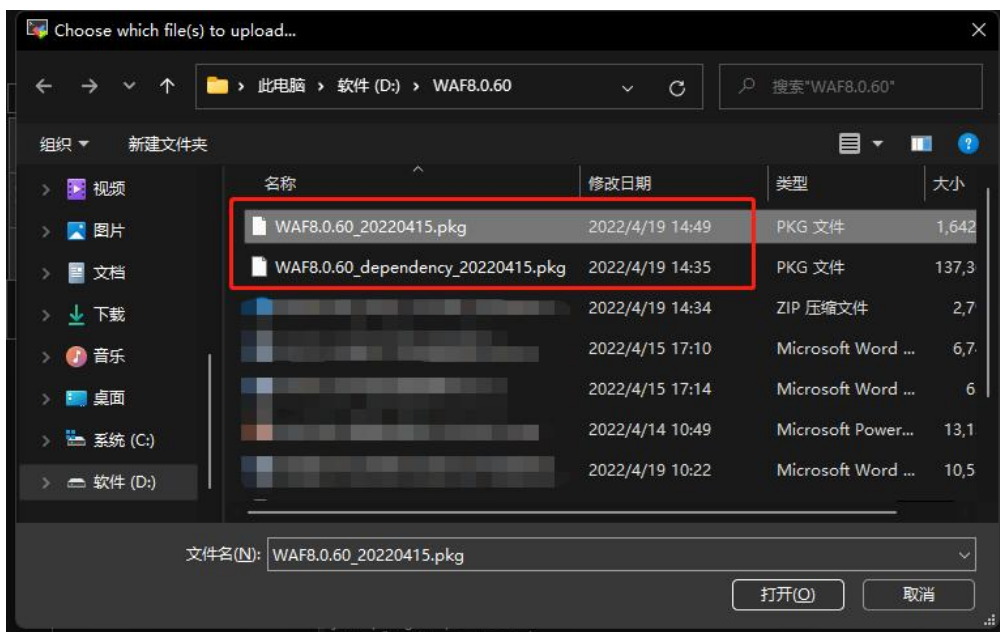

列出所有在运行的容器信息：doker ps

列出本地镜像：docker images

```
[root@waf-fefcfe92b045 tmp]# docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS
21d1d5f7e995   waf_detect:0.60_321b               /bin/sh -c 'chmod +...  22 minutes ago Up 21 minutes 0.0.0.0:6970-6971->6970-6971/tcp, :::6970-6971->6970-6971/tcp
3b3c95e61aa    waf_redis:latest                   /opt/bitnami/script...  22 minutes ago Up 21 minutes 6379/tcp, 127.0.0.1:6381->6381/tcp
c7e49f610c0d   waf_mgt:0.60_321b                  /bin/sh -c 'chmod +...  22 minutes ago Up 21 minutes 0.0.0.0:4431->4431/tcp, :::4431->4431/tcp, 0.0.0.0:20001->20001/tcp, :::20001->20001/tcp
[root@waf-fefcfe92b045 tmp]# docker images
REPOSITORY    TAG       IMAGE ID       CREATED        SIZE
waf_detect    0.60_321b  9491324d639   4 days ago    1.33GB
waf_redis     latest    3d0633623b3   4 days ago    96.1MB
waf_mgt       0.60_321b  7057c099524d  4 days ago    3.38GB
[root@waf-fefcfe92b045 tmp]#
```

3.3.4. 分离式设备插件模式

步骤1. 在宿主机A上，使用远程工具连接Cent OS 7系统，并上传云WAF软件依赖安装包与安装包到/tmp目录下。



步骤2. 在宿主机中，关闭firewalld防火墙和SELinux服务。

- 关闭防火墙：systemctl stop firewalld.service
- 永久关闭防火墙：systemctl disable firewalld.service
- 关闭 SELinux：setenforce 0
- 永久关闭 SELinux：vi /etc/selinux/config，将 SELINUX=enforcing 改为 SELINUX=disabled，并重启设备。

```
[root@qianduoduo ~]# systemctl stop firewalld.service
[root@qianduoduo ~]# systemctl disable firewalld.service
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
```

```
[root@waf-fefcfe40384a tmp]# setenforce 0
setenforce: SELinux is disabled
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

步骤3. 给云WAF的依赖包执行权限。

chmod +x /tmp/[云WAF软件依赖安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_dependency_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 137368
drwx----- 3 root root          17 4月  8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJXSj
-rwxr-xr-x  1 root root    140664292 4月  19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤4. 安装云WAF的依赖包。

若设备能联网优先推荐使用在线安装，无网情况使用离线安装方式。

进入云WAF依赖包存放目录后执行安装命令。

cd /tmp

- 离线：./[云 WAF 软件依赖安装包名]
- 在线：./[云 WAF 软件依赖安装包名] -online

安装时输入 y 确认安装，输入 N 取消安装。

⚠ 注意：

WAF 依赖包安装时，会列表展示出来要卸载和安装的宿主机程序，请确认后再进行下一步。

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_dependency_20220415.pkg -online
Dependencies Resolved

=====
Package Arch Version Size
=====
Installing:
docker-ce x86_64 20.10.10-3.el7 23M
Package Summary
=====
Install 1 dependent packages
Is this ok [y/N]: y

Installing package docker:
已知数据源: fastestmirror, langpacks
正在检查 containerd.io-1.4.11-3.1.el7.x86_64.rpm: 不更新已安装的软件包。
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 3:docker-ce-20.10.10-3.el7.x86_64
docker-ce-20.10.10-3.el7.x86_64.rpm 将被安装
正在检查 docker-ce-cli-20.10.10-3.el7.x86_64.rpm: 3:docker-ce-cli-20.10.10-3.el7.x86_64
docker-ce-cli-20.10.10-3.el7.x86_64.rpm 不更新已安装的软件包。
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: docker-ce-rootless-extras-20.10.10-3.el7.x86_64
docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm 将被安装
正在检查 docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: docker-scan-plugin-0.9.0-3.el7.x86_64
docker-scan-plugin-0.9.0-3.el7.x86_64.rpm 不更新已安装的软件包。
正在解决依赖关系
--> 正在检查事务
--> 软件包 docker-ce.x86_64.3.20.10.10-3.el7 将被 安装
--> 软件包 docker-ce-rootless-extras.x86_64.0.20.10.10-3.el7 将被 安装
--> 解决依赖关系完成

依赖关系解决

=====
Package 架构 版本 源 大小
=====
正在安装:
docker-ce x86_64 3:20.10.10-3.el7 /docker-ce-20.10.10-3.el7.x86_64 96 M
docker-ce-rootless-extras x86_64 20.10.10-3.el7 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64 20 M
=====
事务概要
-----
安装 2 软件包

总计 116 M
安装大小: 116 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
正在安装 : 3:docker-ce-20.10.10-3.el7.x86_64 1/2
正在安装 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 2/2
验证中 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 1/2
验证中 : 3:docker-ce-20.10.10-3.el7.x86_64 2/2
```

步骤5. 安装完成后，执行docker ps查看docker是否运行

```
[root@waf-fefcfe40384a tmp]# docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS    NAMES
[root@waf-fefcfe40384a tmp]# docker images
REPOSITORY    TAG       IMAGE ID   CREATED   SIZE
[root@waf-fefcfe40384a tmp]# ps -aux | grep docker
root          8023      0:0   1.5 1163304 60152 ?        Ssl  15:44   0:00 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root          21231    0:0   0.0 112728   972 pts/0    R+   16:16   0:00 grep --color=auto docker
[root@waf-fefcfe40384a tmp]#
```

步骤6. 安装云WAF安装包，给云WAF安装包执行权限。

chmod +x /tmp/[云WAF安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 1779488
drwx----- 3 root root          17 4月  8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-DUJXSj
-rwxr-xr-x  1 root root 1681526916 4月 19 16:10 WAF8.0.60_20220415.pkg
-rwxr-xr-x  1 root root 140664292 4月 19 15:33 WAF8.0.60_dependency_20220415.pkg
[root@waf-fefcfe40384a tmp]#
```

步骤7. 安装云WAF的安装包，并输入挂载路径和密码

8O#NII@QXIZrW^c&%KPqlc#Y并选择部署角色为Management Platform（管理节点），回车确认。

cd /tmp

./[云WAF安装包名]

注意：安装路径并非一定为/data，可自定义创建文件目录，空间满足大于64G即可

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_20220415.pkg
Please enter the mount path: /data
Please enter the password: *****
Use the arrow keys to navigate: ↓ ↑ → ← and / toggles search
Select Deployment Role
  Management Platform + WAF Agent
  * Management Platform
  WAF Agent

----- Selected Deployment Role -----
Management Platform
```

步骤8. 选择需要部署模式为（插件），回车确认。

```
Write out database with 1 new entries
Data Base Updated
Use the arrow keys to navigate: ↓ ↑ → ← and / toggles search
Select Deployment Method
  Reverse Proxy
  * Plugin

----- Selected Deployment Method -----
Plugin
```

```
Certificate is to be certified until Apr 12 11:05:42 2052 GMT (10950 days)

Write out database with 1 new entries
Data Base Updated
Deployment Method: Plugin
2653d992f4ef: Loading layer
f1affad69343: Loading layer
18a6d2a77388: Loading layer
c377c28a3e43: Loading layer
914120db83a9: Loading layer
8d1dc0b00b3f: Loading layer
360f6aa95169: Loading layer
a93f4df02f78: Loading layer
17fc118b9866: Loading layer
e311caf2fa28: Loading layer
ab2eb94e5e5e: Loading layer
d1d23d2c1f83: Loading layer
62b40dfd1aa3: Loading layer
0268ba6f0efd: Loading layer
Loaded image: waf_detect:8.0.60.321B

216.5MB/216.5MB
181.4MB/181.4MB
150kB/150kB
52.85MB/52.85MB
1.077GB/1.077GB
13.82kB/13.82kB
2.264MB/2.264MB
434.2kB/434.2kB
5.632kB/5.632kB
4.096kB/4.096kB
440.3MB/440.3MB
5.12kB/5.12kB
2.189MB/2.189MB
4.096kB/4.096kB
```

步骤9. 安装成功后，使用以下命令检查安装是否正常，安装成功后，云WAF管理节点会有waf_mgt和waf_redis两个容器正在运行。

列出所有在运行的容器信息：doker ps

列出本地镜像：docker images

```
root@waf-fcf40384a tmp# docker ps
CONTAINER ID        IMAGE                         COMMAND                  CREATED              STATUS              PORTS
00c5ba3f8b7        waf_mgt:8.0.60.321B          /bin/sh -c 'chmod +...   4 minutes ago       Up 4 minutes       0.0.0.0:4431-4431/tcp,...
e54ad295bc        waf_redis:latest           /opt/bitnami/script...   4 minutes ago       Up 4 minutes       6379/tcp, 127.0.0.1:6381-6381/tcp

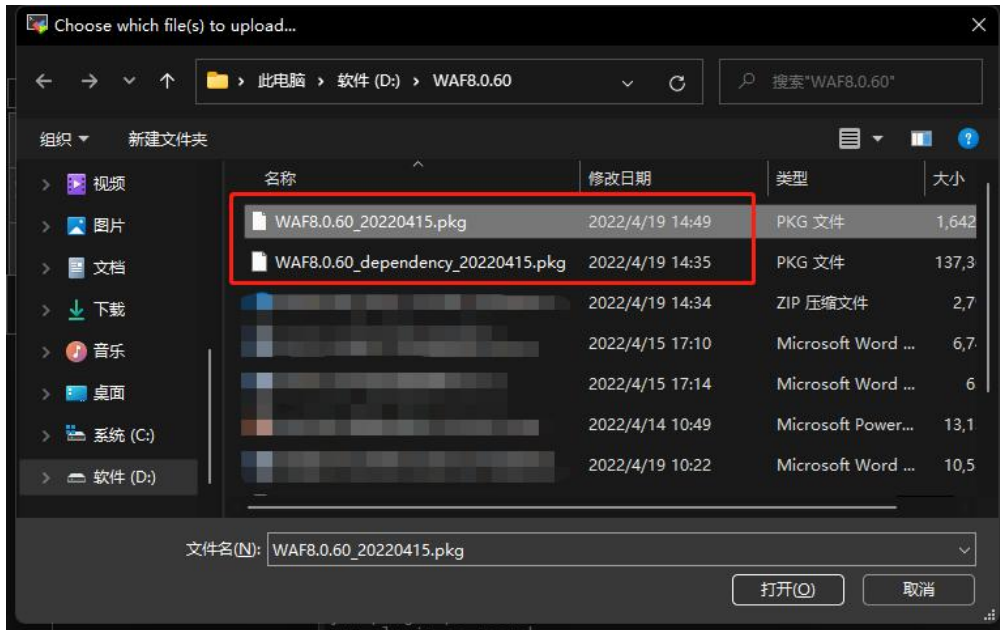
root@waf-fcf40384a tmp# docker images
REPOSITORY        TAG             IMAGE ID          CREATED          SIZE
waf_mgt           8.0.60.321B    8c780b69cfaf     4 days ago      1.6GB
waf_detect        8.0.60.321B    9481b24da639     4 days ago      1.93GB
waf_redis         latest         3d6033233b3     4 days ago      98.1MB
waf_mgt           8.0.60.321B    70c7c099c24d     4 days ago      3.38GB
```

步骤10. 在宿主机A上执行以下命令获取管理节点的证书和Token信息，作为检测节点连接管理节点的凭证。

monitor info

```
root@waf-fcf40384a tmp# monitor info
Deployment Method,
Reverse Proxy,
Deployment Role,
Management Platform
-----Management Platform Configurations-----
https://127.0.0.1:4431
Management Platform Communication Certificate
-----
-----
-----
```

步骤11. 在宿主机B上，使用远程工具连接Cent OS 7系统，并上传云WAF软件依赖安装包与安装包到tmp目录下。



步骤12. 在宿主机B中，关闭firewalld防火墙和SELinux服务。

- 关闭防火墙：systemctl stop firewalld.service
- 永久关闭防火墙：systemctl disable firewalld.service
- 关闭 SELinux：setenforce 0
- 永久关闭 SELinux：vi /etc/selinux/config，将 SELINUX=enforcing 改为 SELINUX=disabled，并重启设备。

```
[root@qianduoduo ~]# systemctl stop firewalld.service
[root@qianduoduo ~]# systemctl disable firewalld.service
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
```

```
[root@waf-fefcfe40384a tmp]# setenforce 0
setenforce: SELinux is disabled
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

步骤13. 给云WAF的依赖包执行权限。

chmod +x /tmp/[云WAF软件依赖安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_dependency_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 137368
drwxr-xr-x 3 root root    17 4月  8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJXsj
-rwxr-xr-x 1 root root 140664292 4月 19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤14. 安装云WAF的依赖包。

若设备能联网优先推荐使用在线安装，无网情况使用离线安装方式。

进入云WAF依赖包存放目录后执行安装命令。

cd /tmp

- 离线：./[云 WAF 软件依赖安装包名]
- 在线：./[云 WAF 软件依赖安装包名] -online

安装时输入 y 确认安装，输入 N 取消安装。

⚠ 注意：

WAF 依赖包安装时，会列表展示出要卸载和安装的宿主主机程序，请确认后再进行下一步。

```
[root@waf-fefcfe40384a tmp]# ./WAF8.0.60_dependency_20220415.pkg -online
Dependencies Resolved
-----
Package Arch Version Size
-----
Installing:
docker-ce x86_64 20.10.10-3.el7 23M
-----
Package Summary
-----
Install 1 dependent packages
Is this ok [Y/n]: y
-----
Install rpm package docker:
正在检查 rpm 包 fastestairroot langpacks
正在检查 containerd.io-1.4.11-3.1.el7.x86_64.rpm: containerd.io-1.4.11-3.1.el7.x86_64
正在检查 containerd.io-1.4.13-3.1.el7.x86_64.rpm: 需要新安装的软件包。
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 3:docker-ce-20.10.10-3.el7.x86_64
正在检查 docker-ce-20.10.10-3.el7.x86_64.rpm: 需要安装
正在检查 docker-ce-cli-20.10.10-3.el7.x86_64.rpm: 1:docker-ce-cli-20.10.10-3.el7.x86_64
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: 需要新已安装的软件包。
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: 需要安装
正在检查 docker-ce-rootless-extras-20.10.10-3.el7.x86_64.rpm: 需要安装
正在检查 docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: docker-scan-plugin-0.9.0-3.el7.x86_64
正在检查 docker-scan-plugin-0.9.0-3.el7.x86_64.rpm: 需要新已安装的软件包。
正在解决依赖关系
--> 正在检查事务
--> 软件包 docker-ce.x86_64.3.20.10.10-3.el7 将被 安装
--> 软件包 docker-ce-rootless-extras.x86_64.0.20.10.10-3.el7 将被 安装
--> 解决依赖关系完成

依赖关系解决
-----
Package 架构 版本 源 大小
-----
正在安装:
docker-ce x86_64 3:20.10.10-3.el7 /docker-ce-20.10.10-3.el7.x86_64 96 M
docker-ce-rootless-extras x86_64 0:20.10.10-3.el7 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64 20 M
-----
事务概要
-----
安装 2 软件包
总计 116 M
安装大小 116 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
正在安装 : 3:docker-ce-20.10.10-3.el7.x86_64 1/2
正在安装 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 2/2
验证中 : docker-ce-rootless-extras-20.10.10-3.el7.x86_64 1/2
验证中 : 3:docker-ce-20.10.10-3.el7.x86_64 2/2
```

步骤15. 安装完成后，执行docker ps查看docker是否运行

```
[root@waf-fefcfe40384a tmp]# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
[root@waf-fefcfe40384a tmp]# docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
[root@waf-fefcfe40384a tmp]# ps -aux | grep docker
root 8023 0.0 1.5 1163304 60152 ? Ssl 15:44 0:00 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root 21231 0.0 0.0 112728 972 pts/0 R+ 16:16 0:00 grep --color=auto docker
[root@waf-fefcfe40384a tmp]#
```

步骤16. 安装云WAF安装包，给云WAF安装包执行权限。

chmod +x /tmp/[云WAF安装包名]

```
[root@waf-fefcfe40384a tmp]# chmod +x WAF8.0.60_20220415.pkg
[root@waf-fefcfe40384a tmp]# ll
总用量 1779488
drwx----- 3 root root 17 4月 8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJXSj
-rwxr-xr-x 1 root root 1681526916 4月 19 16:10 WAF8.0.60_20220415.pkg
-rwxr-xr-x 1 root root 140664292 4月 19 15:33 WAF8.0.60_dependency_20220415.pkg
```

步骤17. 安装云WAF的安装包，并输入挂载路径和密码

80#NII@QXIZrW^c&%KPqIc#Y并选择部署角色为WAF Agent（检测节点），回车确认。

cd /tmp

./[云WAF安装包名]


```
root@5a7b541159f4:/# cat /etc/nginx/nginx.conf
user nginx;
worker_processes auto;

error_log /var/log/nginx/error.log notice;
pid /var/run/nginx.pid;
load_module /etc/nginx/nginx_1.21.6_http_waf_agent_module.so;

events {
    worker_connections 1024;
}

http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    sendfile on;
    #tcp_nopush on;

    keepalive_timeout 65;

    #gzip on;

    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/template.conf;
}
root@5a7b541159f4:/#
```

步骤21. 根据实际云WAF部署情况，修改template.conf引流配置文件。server配置表示把经过此nginx的流量引流到云WAF检测节点进行业务防护，填写的server IP为云WAF检测节点的IP，端口默认从6970开始依次递增，一个检测节点有多少核CPU，就可以配置多少个端口，如下图为2核的检测节点。

```
root@5a7b541159f4:/# cat /etc/nginx/template.conf
upstream waf_server {
    hash $remote_addr$remote_port;
    keepalive 512;

    #custom by cpu nums
    server 10.243.3.88:6970;
    server 10.243.3.88:6971;
}

waf_agent /waf_detect;
waf_agent_request_body_max_size 1m;
waf_filter /waf_detect;
waf_filter_buffer 1m;
waf_filter_reply_body_max_size 1m;

server_include {
    location /waf_detect {
        internal;
        waf_pass waf_server;
        waf_pass_connect_timeout 1s;
        waf_pass_read_timeout 1s;
        waf_pass_send_timeout 1s;
    }
}
root@5a7b541159f4:/#
```

⚠ 注意:

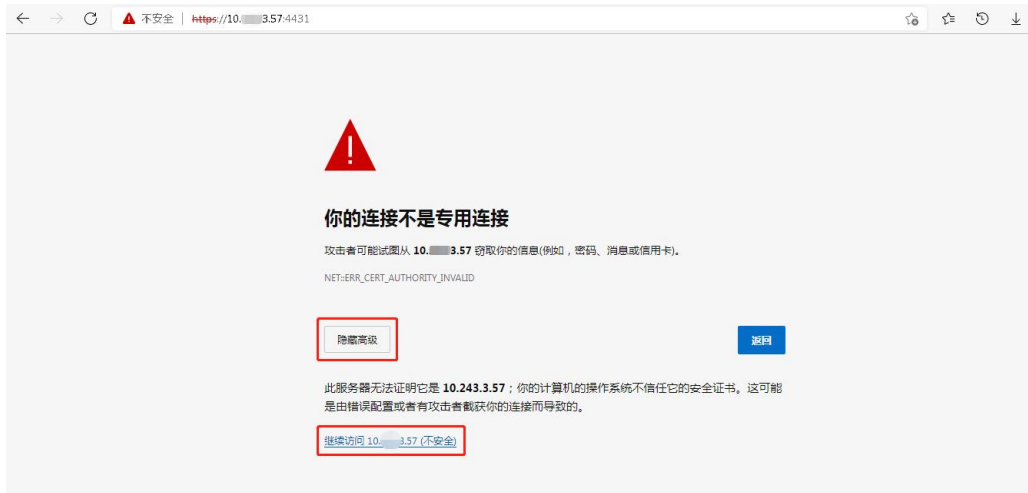
一个 nginx 可以配置多个检测节点的 IP。例如部署了 2 个 WAF 检测节点，一台检测节点有 2 核 CPU，一台检测节点有 4 核 CPU，则配置如下：

```
#custom by cpu nums
server 10.246.84.125:6970;
server 10.246.84.125:6971;
server 10.246.84.126:6970;
server 10.246.84.126:6971;
server 10.246.84.126:6972;
server 10.246.84.126:6973;
```

步骤22. 配置完插件后，重新启动nginx服务，让引流插件才能生效。

3.4. 登录云 WAF

步骤1. 在浏览器中输入<https://管理节点IP:4431>打开云WAF的登录页面，若浏览器出现不授信的告警，点击<高级/继续访问>。



步骤2. 云WAF的默认账号密码为admin/admin



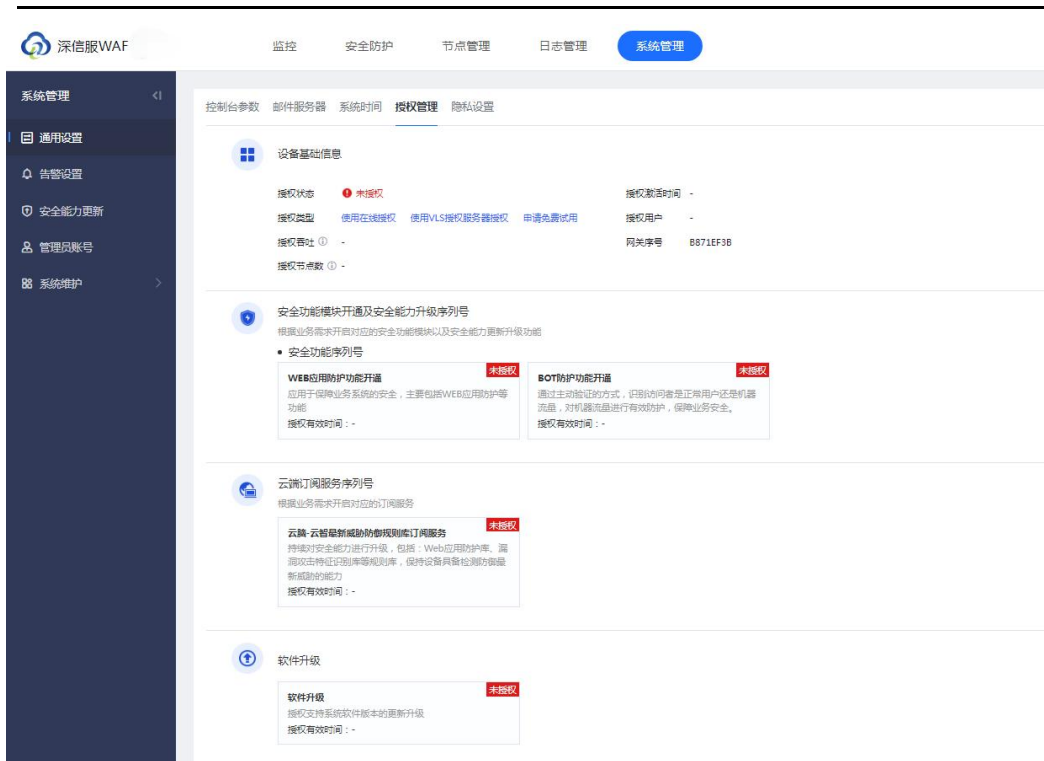
3.5. 云 WAF 授权

云WAF授权分为三种“在线授权”、“本地授权服务器授权”和“申请免费试用”。

- 在线授权：需要先购买获得序列号，然后将序列号信息填写到对应的位置；
- 本地授权服务器授权：需要在本地搭建一个授权服务器（VLS），使用授权服务器对云 WAF 来授权；
- 申请试用：只要填写申请信息即可通过短信方式获得授权序列号，把序列号填入在线授权即可，使用此序列号可以免费试用 30 天。

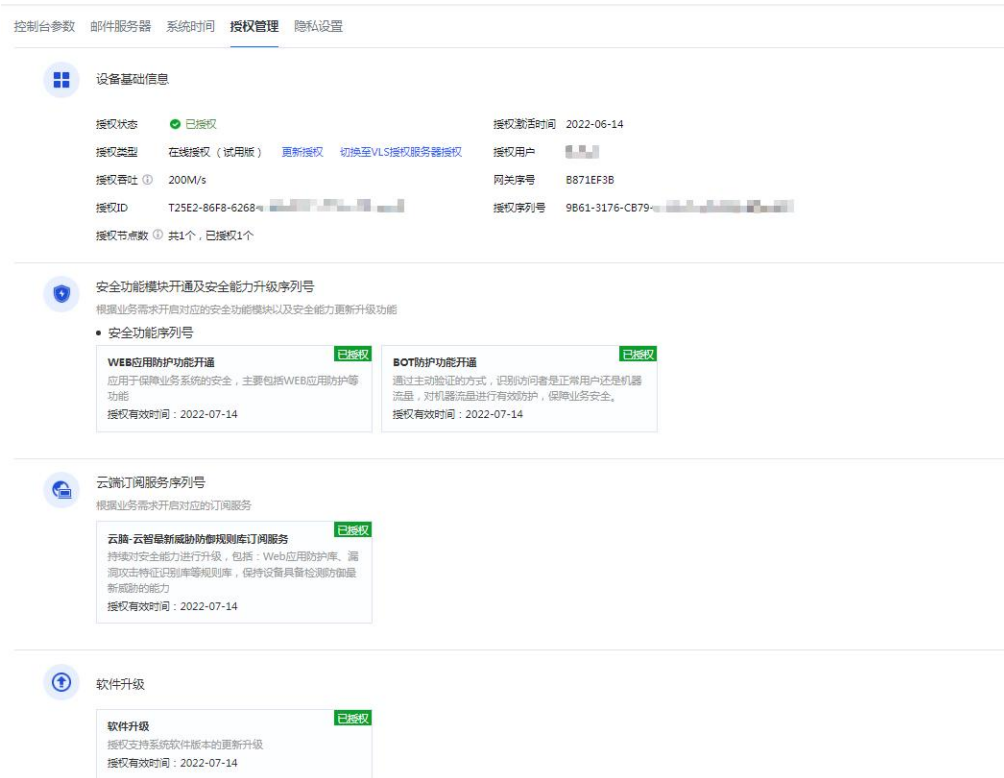
说明：

使用“在线授权”与“申请免费试用”的授权方式都需要云 WAF 能够连接互联网，与 vls.sangfor.com.cn 的 TCP 443 端口保持通信。



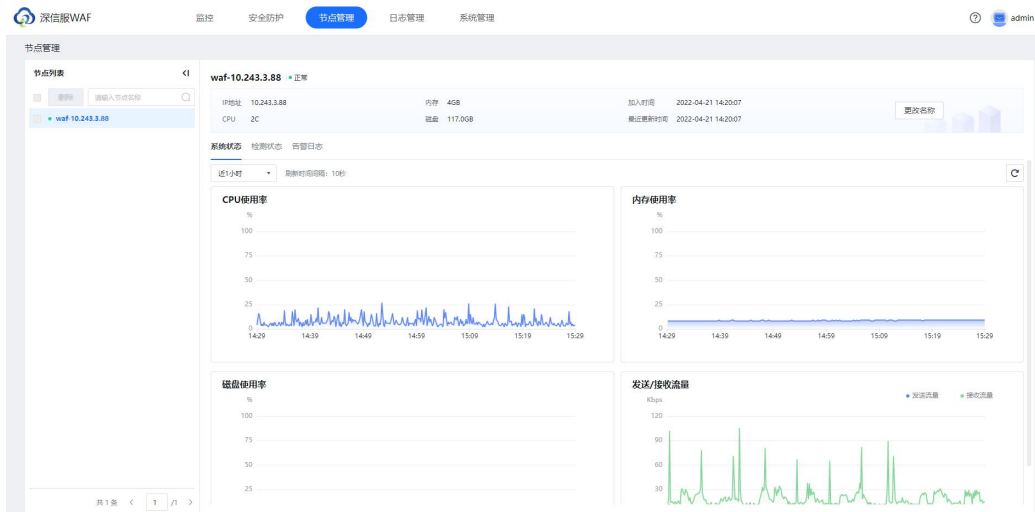
授权完成后可以在[系统管理/通用设置/授权管理]中看到详细的授权情况。分离式设备仅需管理节点授权即可，检测节点无需授权。

- 授权吞吐：设备支持最大应用层吞吐。
- 授权节点数：检测节点接入管理节点个数。



3.6. 检查检测节点是否上线

在云WAF管理平台控制台[节点管理]中查看节点是否上线。

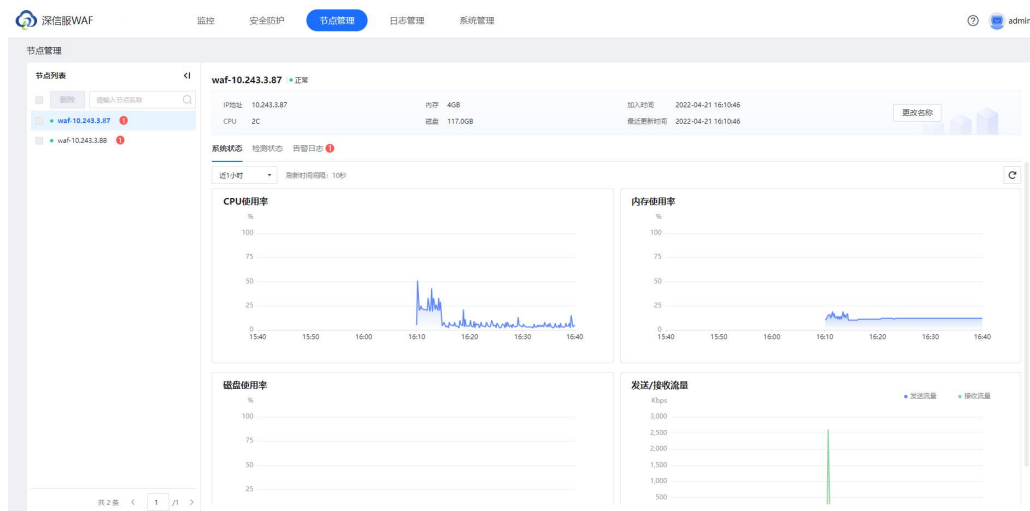


3.7. 集群部署

3.7.1. 分离式设备反向代理模式集群

分离式设备反向代理模式集群需要有一个管理节点和两个及以上的检测节点，且前置负载均衡设备。

步骤1. 在云WAF管理平台控制台[节点管理]中查看所有节点是否上线。



步骤2. 在云WAF设备上配置站点防护，具体案例可参考[4.1章节](#)。

序号	健康状态	站点名称	防护域名	服务类型	监听端口	WEB防护策略	BOT防护策略	启用/禁用	操作
1	正常	门户网站	10.0.0.57	http	80	WEB防护策略	BOT防护策略	启用	编辑 复制 删除

说明:

云WAF的安全策略建议开启真实客户端IP识别X-Forwarded-For，并将负载均衡设备地址填写到代理服务器IP中，避免云WAF封堵IP为负载均衡设备的IP从而影响正常业务。

步骤3. 在负载均衡设备（以深信服应用交付AD为例）上，在[应用负载/节点池]中新增节点池，将检测节点添加到节点池中，节点选择策略选择基于源IP哈希的策略，IP为云WAF的检测节点IP，端口填写云WAF监听端口，健康检查选择connect_tcp的策略（可根据实际情况选择），会话保持基于源IP的会话保持策略（可根据实际情况选择）。

名称:

描述:

节点选择策略:

哈希

按优先级调度:

启用
 禁用

哈希字段:

SRC_IP

节点:

IP

输入域名、IPv4/IPv6地址或用“”连接的IP范围

端口:

输入端口

添加

选择节点:

✕ 删除

<input type="checkbox"/>	类型	IP地址	端口	权重	优先级	操作
<input type="checkbox"/>	IP	10.243.3.87	80	-	-	编辑 删除
<input type="checkbox"/>	IP	10.243.3.88	80	-	-	编辑 删除

当前已配置 2 条记录

健康检查

健康检查方法: 已选择 (1/5) 新增

connect_tcp

待选 (38) 刷新 请输入

- TCP被动
- ping
- ping6
- connect_udp
- http
- ftp
- pop3

节点有效条件: 常规检查方法 全部

节点恢复方法: 手动恢复 定时恢复 3 分钟

⚠ 注意:

注意负载均衡设备的调度策略选择，原则是需要把同一用户流量负载到同一个云 WAF 的检测节点上，否则可能影响安全检测效果。

步骤4. 在负载均衡设备（以深信服应用交付AD为例）上，在[应用负载/优化策略/HTTP优化策略]中新增优化策略，启用透传IP到服务器中，传输类型选择传输客户端IP至后台服务器，HTTP头部名称配置为X-Forwarded-For。

HTTP优化策略 ✕

名称:

描述:

HTTP缓存

HTTP缓存: 启用 禁用

HTTP压缩

HTTP压缩: 启用 禁用

其它

透传IP到服务器: 启用 禁用

传输类型: ▼

HTTP头部名称:

步骤5. 在负载均衡设备（以深信服应用交付AD为例）上，在[应用负载/虚拟服务]中新增虚拟服务。服务类型选择HTTP/HTTPS，IP地址和端口设置为负载均衡设备需要反向代理的IP和端口，默认节点池选择云WAF的检测节点池，HTTP优化策略选择步骤4创建的透传IP策略。

虚拟服务

基本信息

名称:

描述:

启/禁用: 启用 禁用

服务类型: ▼

IP地址: ⓘ

端口范围: ⓘ

入口链路: 所有链路 指定链路

默认节点池: ▼

SNAT策略: ▼

源端口策略: ▼ ⓘ

[+ 隐藏以下配置](#)

优化策略

HTTP优化策略: 透传客户端IP ▼ 新增

HTTP2策略: NONE ▼ 新增

TCP策略: NONE ▼ 新增

安全策略

HTTP防护策略: NONE ▼ 新增

QoS策略: NONE ▼ 新增

说明:

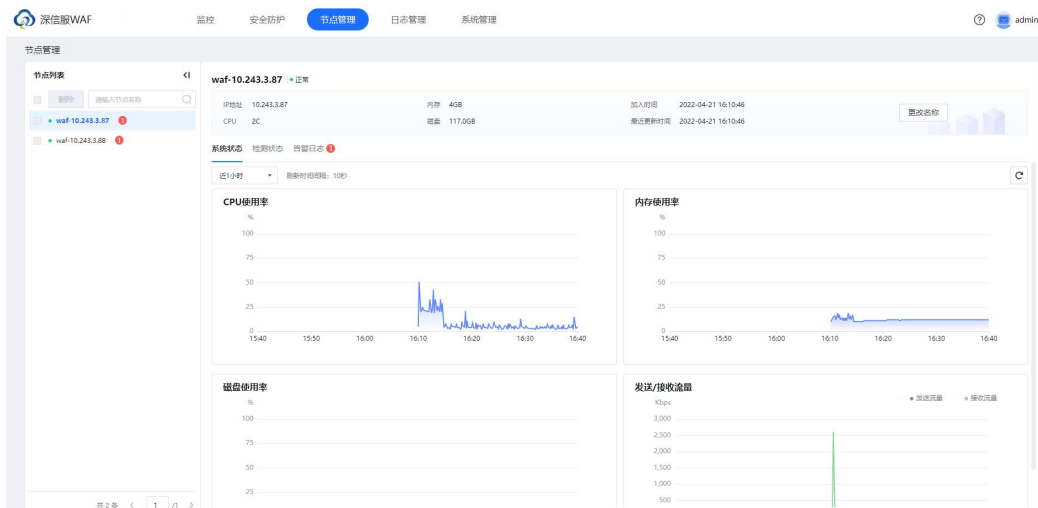
若是 SSL 卸载场景，则 SSL 卸载功能配置负载均衡设备上，云 WAF 的反向代理协议选择 HTTP 协议。

步骤6. 若后续有其他业务需要负载，重复以上步骤即可。

3.7.2. 分离式设备插件模式集群

分离式设备插件模式集群需要有一个管理节点和两个及以上的检测节点。

步骤1. 在云WAF管理平台控制台[节点管理]中查看所有节点是否上线。



步骤2. 在Nginx反向代理服务器上修改云WAF插件的template.conf引流配置文件，添加server字段。填写的server IP为云WAF检测节点的IP，端口默认从6970开始依次递增，一个检测节点有多少核CPU，就可以配置多少个端口。

```
upstream waf_server {
    hash $remote_addr$remote_port;
    keepalive 512;

    #custom by cpu nums
    server 10.243.3.87:6970;
    server 10.243.3.87:6971;
    server 10.243.3.88:6970;
    server 10.243.3.88:6971;
}

waf_agent /waf_detect;
waf_agent_request_body_max_size 1m;
waf_filter /waf_detect;
waf_filter_buffer 1m;
waf_filter_reply_body_max_size 1m;

server_include {
    location /waf_detect {
        internal;
        waf_pass waf_server;
        waf_pass_connect_timeout 1s;
        waf_pass_read_timeout 1s;
        waf_pass_send_timeout 1s;
    }
}
```

 **说明：**

存在多个 server 节点，云 WAF 插件默认使用基于源 IP 和端口的哈希做负载调度算法，不建议进行修改，否则可能影响安全检测效果。

步骤3. 修改完成后重启Nginx服务器即可。

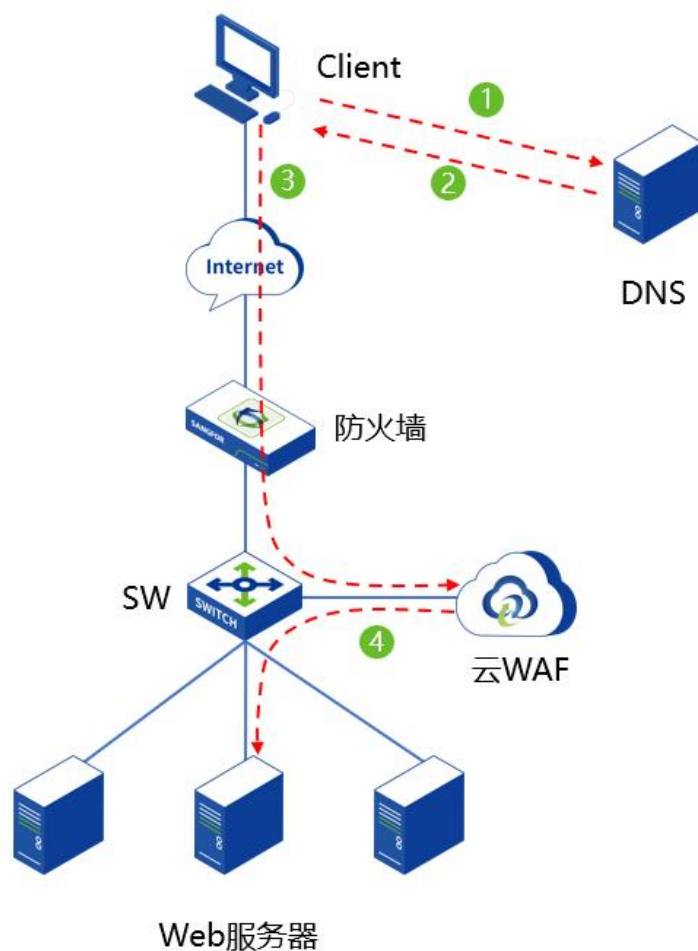
4. 基本功能配置

4.1. 反向代理模式

4.1.1. HTTP 站点防护配置案例

4.1.1.1. 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。

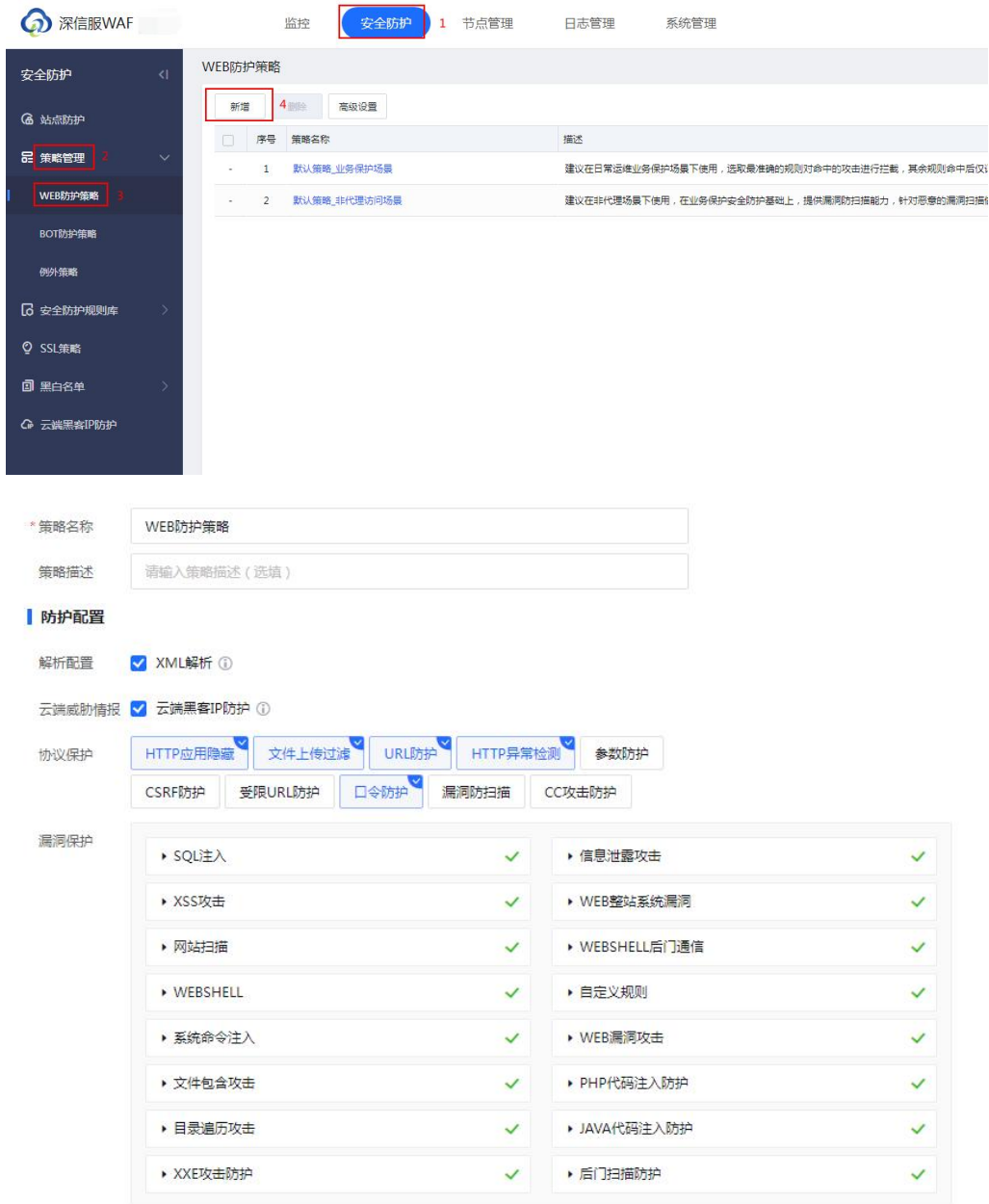


4.1.1.2. 需求分析

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。

4.1.1.3. 配置步骤

步骤1. 在设备[安全防护/策略管理/WEB防护策略]中创建Web服务器的WEB防护策略，也可以直接复用默认策略模板。



步骤2. 在设备[安全防护/站点防护]中创建站点防护。



步骤3. 创建需要防护地址的相关参数。

序号	参数	说明
01	站点名称	配置进行代理防护的 Web 站点的策略名称。
02	防护域名	需要防护的站点域名，支持 IP 地址和域名两种形式。 <ul style="list-style-type: none"> ● 填写 IP 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是 IP 地址，有内网使用私有 IP 访问需求，则填写云 WAF 宿主机 IP 地址；有互联网访问需求，则填写云 WAF 宿主机 IP 映射后的公网 IP 地址；若既有私有 IP 地址访问需求，也有公网 IP 地址访问需求，则均需填写。 ● 填写域名 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是域名，则域名的 DNS 解析需要解析成云 WAF 宿主机的 IP 地址或 NAT 映射后的地址。
03	服务类型	云 WAF 支持对 http 和 https 协议进行反向代理和安全防护。
04	监听端口	云 WAF 进行反向代理所监听的端口。 支持单个端口或端口范围（如：80-88）后，最多可以添加 16 个。
05	备注	对此防护策略进行备注描述，可留空。
06	负载调度算法	云 WAF 反向代理支持负载均衡算法调度，分别有[加权最小连接]、[源地址哈希]、[轮询]三种。 <ul style="list-style-type: none"> ● 加权最少连接 表示选择（连接数/权重）最小的节点。 ● 源地址哈希 根据源 IP 经过哈希运算得到哈希值，使不同的源 IP 尽可能平均调度节点池中各个节点，相同源 IP 的访问调度到同一个节点。 ● 轮询 表示交替返回有效的节点。
07	转发服务器	云 WAF 反向代理的真实服务器的地址。

08	启用健康检查	对转发服务器中的节点进行服务状态检查，支持 http/https/tcp 的检查方式，并且可以自定义检查的阈值。
09	保持连接方式	<ul style="list-style-type: none"> ● 短连接 浏览器和服务器每进行一次 HTTP 操作，就建立一次连接，但任务结束就中断连接。在 HTTP/1.0 中，默认使用的是短连接。 ● 长连接 浏览器和服务器进行一次 HTTP 操作后，浏览器和服务器之间用于传输 HTTP 数据的 TCP 连接不会关闭，如果客户端再次访问这个服务器上的网页，会继续使用这一条已经建立的连接。从 HTTP/1.1 起，默认使用长连接。 云 WAF 默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接。
10	会话保持	会话保持是基于 Cookie 的会话保持方式，该方式匹配 HTTP 请求中的 Cookie 字段，通过不同 Cookie 区分不同客户端，可以将所有携带相同 Cookie 的 HTTP 流量转发到同一个转发服务器上面。并且可自定义设置会话保持时间，0 表示浏览器关闭时 cookie 失效，最大 24 小时。
11	X-Forwarded-For	<p>X-Forwarded-For 实现了云 WAF 到服务器之间的客户端真实地址透传，后端服务器识别 X-Forwarded-For 字段可以知道访问客户端的真实 IP 地址。</p> <ul style="list-style-type: none"> ● 在末尾追加上一跳的 IP 地址 在 HTTP 头部追加插入 X-Forwarded-For 字段，为上一跳的 IP 地址。 ● 原封不动 不插入 X-Forwarded-For 字段。 ● 用上一跳的 IP 地址覆盖原有内容 在 HTTP 头部插入 X-Forwarded-For 字段，为上一跳的 IP 地址。若 HTTP 头部存在 X-Forwarded-For 字段，则用上一跳的 IP 地址覆盖原有内容。
12	头部改写	可以对 HTTP 的请求头、相应头进行添加或是隐藏相关参数。
13	WEB 防护策略	调用创建的 WEB 防护策略，若选择暂不使用 WEB 防护策略，则只对站点进行反向代理，不进行 WEB 安全防护。
14	BOT 防护策略	调用创建的 BOT 防护策略，若选择暂不使用 BOT 防护策略，则只对站点进行反向代理，不进行 BOT 安全防护。
15	检测动作	检查动作分为“检测后放行”、“检测后拦截”两种。
16	联动封锁	<p>联动封锁分为“高危行为联动封锁”、“任意攻击行为联动封锁”两种。</p> <ul style="list-style-type: none"> ● 高危行为联动封锁 仅封锁具有高危行为特征的 IP，优先保证用户流畅上网、业务稳定的提供服务。 ● 任意攻击行为联动封锁 对任意具有攻击特征的 IP 执行访问封锁，最大化业务和用户的安全防御能力。 注意：开启联动封锁可有效阻断攻击者的后续攻击力，同时当业务系统代码不规范导致误判发生时，可能会引起业务无法访问。
17	请求检测	检测 http/https 的请求 body 大小，最大支持 10M。

18	响应检测	检测 http/https 的相应 body 大小，最大支持 10M。
19	真实客户端 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，请在此填写代理头部字段和真实源 IP 的层数，用于识别真实的源 IP 进行日志记录和封锁；同时请关闭中低频 WEB 口令爆破防护，以防止误封锁代理 IP。
20	代理服务器 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，在此填写 CDN IP 或代理 IP，用于进行日志记录和联动封锁。

基础信息

* 站点名称

* 防护域名

* 服务类型 http https

* 监听端口 ×
输入单个端口或端口范围（如：80-88）后，按Enter键添加。最多可以添加16个

备注

请求信息

* 负载调度算法 加权最小连接 源地址哈希 轮询

* 转发服务器 : ×
 : ×

启用健康检查 [设置](#)

* 保持连接方式 短连接 长连接
默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接

会话保持 启用会话保持

会话保持时间 ①

* X-Forwarded-For

头部改写

<input type="checkbox"/>	类型	动作	参数名	参数值	操作
暂无数据					

防护方式

* BOT防护策略

* WEB防护策略

* 检测动作 检测后放行 检测后拦截

联动封锁 启用联动封锁

* 请求检测 请求检测body大小 KB

响应检测 启用响应检测

响应检测body大小 KB

真实客户端IP

<input type="checkbox"/>	头部字段	IP层数	操作
暂无数据			

代理服务器IP

步骤4. 配置完成后，点击<确定>即可完成配置。

新增	应用	禁用	删除	全部健康状态	全部WEB防护策略	全部BOT防护策略	站点名称/域名/监听端口	操作		
<input type="checkbox"/>	序号	健康状态	站点名称	防护域名	服务类型	监听端口	WEB防护策略	BOT防护策略	启用/禁用	操作
<input type="checkbox"/>	1	未检测	门户网站	a.sangfor.com	http	80	WEB防护策略	暂不使用BOT策略	<input checked="" type="checkbox"/>	编辑 复制 删除

步骤5. 若站点使用域名，则需要域名的解析修改成云WAF宿主机（单台设备部署）/云WAF检测节点（分离式设备部署）的地址。

修改记录 X

记录类型: A- 将域名指向一个IPV4地址 v

主机记录: 1.2.3.4.5.6 .dns-example.com ?

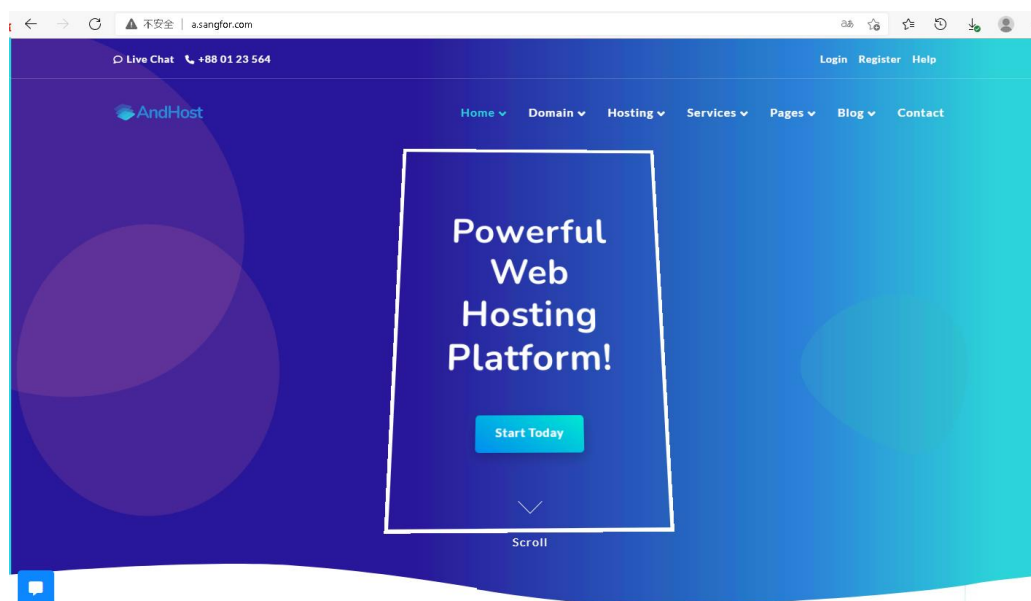
解析线路: 默认 - 必填! 未匹配到智能解析线路时, 返回【默认】线路... ?

* 记录值: 5.5.5.5

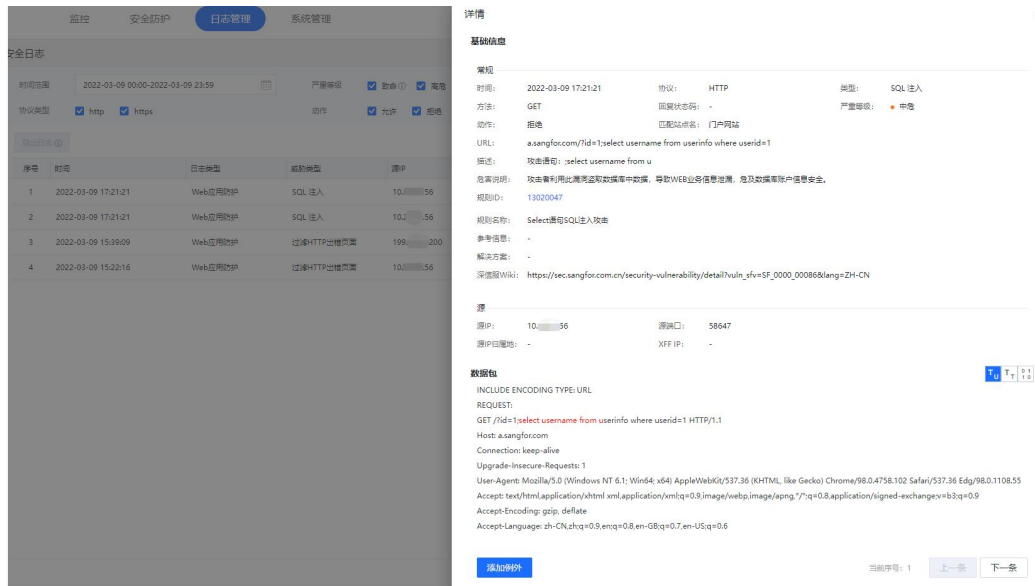
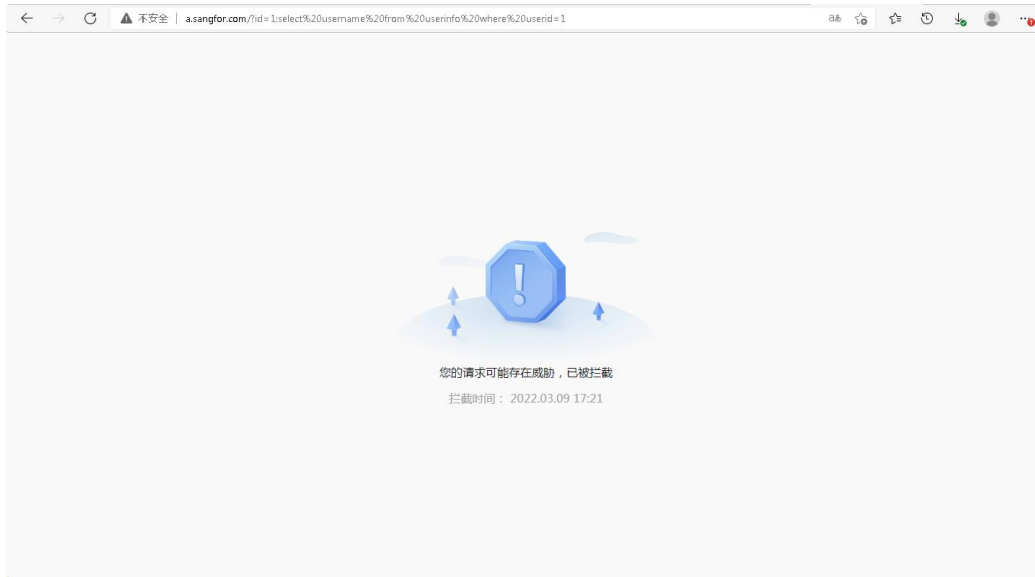
* TTL: 10 分钟 v

4.1.1.4. 效果预览

使用浏览器访问站点，可以成功访问到配置的http服务器站点。



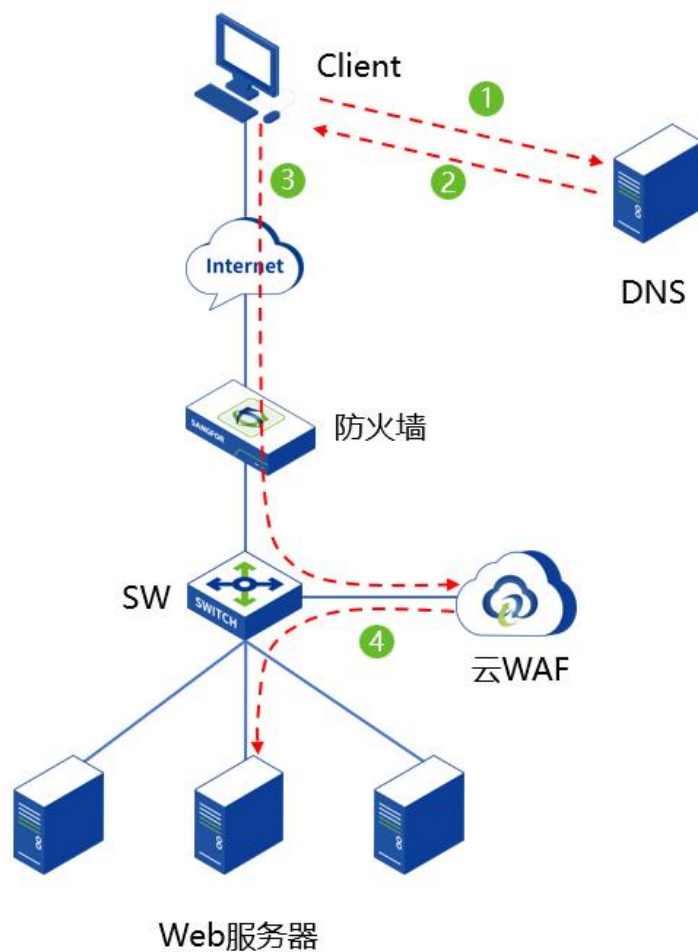
模拟进行攻击，成功拦截，并可以查询到安全日志。



4.1.2. HTTPS 站点防护配置案例_HTTTPS 解密

4.1.2.1. 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HTTTPS。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。



4.1.2.2. 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。

4.1.2.3. 配置步骤

步骤1. 在设备[安全防护/策略管理/WEB防护策略]中创建Web服务器的WEB防护策略，也可以直接复用默认策略模板。

WEB防护策略

新增 4 删除 高级设置

序号	策略名称	描述
1	默认策略_业务保护场景	建议在日运营业务保护场景下使用，选取最准确的规则对命中攻击进行拦截，其余规则命中后仅
2	默认策略_非代理访问场景	建议在非代理场景下使用，在业务保护安全防护基础上，提供漏扫扫描能力，针对恶意的漏扫扫描

*策略名称: WEB防护策略

策略描述: 请输入策略描述 (选填)

防护配置

解析配置 XML解析

云端威胁情报 云端黑客IP防护

协议保护: HTTP应用隐藏, 文件上传过滤, URL防护, HTTP异常检测, 参数防护

CSRF防护, 受限URL防护, 口令防护, 漏洞防扫描, CC攻击防护

漏洞保护

SQL注入	✓	信息泄露攻击	✓
XSS攻击	✓	WEB整站系统漏洞	✓
网站扫描	✓	WEBSHELL后门通信	✓
WEBSHELL	✓	自定义规则	✓
系统命令注入	✓	WEB漏洞攻击	✓
文件包含攻击	✓	PHP代码注入防护	✓
目录遍历攻击	✓	JAVA代码注入防护	✓
XXE攻击防护	✓	后门扫描防护	✓

步骤2. 在设备[安全防护/SSL策略/证书管理]中点击<新增>，导入SSL证书。

深信服WAF 安全防护 1 节点管理 日志管理 系统管理

SSL策略管理 证书管理 3

新增 4 删除

序号	名称	签发时间	过期时间
1	默认证书	2021年10月6日 16:42:44	2031年10月4日 16:42:44

新增服务器证书

*名称

描述

*颁发类型 导入证书文件 导入一对公私钥

*选择证书文件

密码

步骤3. 在设备[安全防护/SSL策略/SSL策略管理]中点击<新增>，添加SSL策略，选择导入的服务器证书，及启用的SSL协议和加密算法。



新增SSL策略

*名称

描述

*服务器证书

*启用协议 TLS1.0 TLS1.1 TLS1.2 TLS1.3

*加密算法

已选 (18 / 18)

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

待选 (0)

步骤4. 在设备[安全防护/站点防护]中创建站点防护。



步骤5. 创建需要防护地址的相关参数。

序号	参数	说明
01	站点名称	配置进行代理防护的 Web 站点的策略名称。
02	防护域名	<p>需要防护的站点域名，支持 IP 地址和域名两种形式。</p> <ul style="list-style-type: none"> ● 填写 IP 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是 IP 地址，有内网使用私有 IP 访问需求，则填写云 WAF 宿主机 IP 地址；有互联网访问需求，则填写云 WAF 宿主机 IP 映射后的公网 IP 地址；若既有私有 IP 地址访问需求，也有公网 IP 地址访问需求，则均需填写。 ● 填写域名 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是域名，则域名的 DNS 解析需要解析成云 WAF 宿主机的 IP 地址或 NAT 映射后的地址。
03	服务类型	云 WAF 支持对 http 和 https 协议进行反向代理和安全防护。
04	监听端口	云 WAF 进行反向代理所监听的端口。 支持单个端口或端口范围（如：80-88）后，最多可以添加 16 个。
05	备注	对此防护策略进行备注描述，可留空。
06	负载调度算法	<p>云 WAF 反向代理支持负载均衡算法调度，分别有[加权最小连接]、[源地址哈希]、[轮询]三种。</p> <ul style="list-style-type: none"> ● 加权最少连接 表示选择（连接数/权重）最小的节点。 ● 源地址哈希 根据源 IP 经过哈希运算得到哈希值，使不同的源 IP 尽可能平均调度节点池中各个节点，相同源 IP 的访问调度到同一个节点。 ● 轮询 表示交替返回有效的节点。
07	转发服务器	云 WAF 反向代理的真实服务器的地址。

08	启用健康检查	<p>对转发服务器中的节点进行服务状态检查，支持 http/https/tcp 的检查方式，并且可以自定义检查的阈值。</p> <p>注意：https 仅支持 SSLv3 协议，使用其他协议如 TLS1.2、TLS1.3 建议使用 tcp 的健康检查。</p>
09	保持连接方式	<ul style="list-style-type: none"> ● 短连接 <p>浏览器和服务器每进行一次 HTTP 操作，就建立一次连接，但任务结束就中断连接。在 HTTP/1.0 中，默认使用的是短连接。</p> <ul style="list-style-type: none"> ● 长连接 <p>浏览器和服务器进行一次 HTTP 操作后，浏览器和服务器之间用于传输 HTTP 数据的 TCP 连接不会关闭，如果客户端再次访问这个服务器上的网页，会继续使用这一条已经建立的连接。从 HTTP/1.1 起，默认使用长连接。</p> <p>云 WAF 默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接。</p>
10	会话保持	<p>会话保持是基于 Cookie 的会话保持方式，该方式匹配 HTTP 请求中的 Cookie 字段，通过不同 Cookie 区分不同客户端，可以将所有携带相同 Cookie 的 HTTP 流量转发到同一个转发服务器上面。并且可自定义设置会话保持时间，0 表示浏览器关闭时 cookie 失效，最大 24 小时。</p>
11	X-Forwarded-For	<p>X-Forwarded-For 实现了云 WAF 到服务器之间的客户端真实地址透传，后端服务器识别 X-Forwarded-For 字段可以知道访问客户端的真实 IP 地址。</p> <ul style="list-style-type: none"> ● 在末尾追加上一跳的 IP 地址 <p>在 HTTP 头部追加插入 X-Forwarded-For 字段，为上一跳的 IP 地址。</p> <ul style="list-style-type: none"> ● 原封不动 <p>不插入 X-Forwarded-For 字段。</p> <ul style="list-style-type: none"> ● 用上一跳的 IP 地址覆盖原有内容 <p>在 HTTP 头部插入 X-Forwarded-For 字段，为上一跳的 IP 地址。若 HTTP 头部存在 X-Forwarded-For 字段，则用上一跳的 IP 地址覆盖原有内容。</p>
12	头部改写	<p>可以对 HTTP 的请求头、相应头进行添加或是隐藏相关参数。</p>
13	WEB 防护策略	<p>调用创建的 WEB 防护策略，若选择暂不使用 WEB 防护策略，则只对站点进行反向代理，不进行 WEB 安全防护。</p>
14	BOT 防护策略	<p>调用创建的 BOT 防护策略，若选择暂不使用 BOT 防护策略，则只对站点进行反向代理，不进行 BOT 安全防护。</p>
15	检测动作	<p>检查动作分为“检测后放行”、“检测后拦截”两种。</p>
16	联动封锁	<p>联动封锁分为“高危行为联动封锁”、“任意攻击行为联动封锁”两种。</p> <ul style="list-style-type: none"> ● 高危行为联动封锁 <p>仅封锁具有高危行为特征的 IP，优先保证用户流畅上网、业务稳定的提供服务。</p> <ul style="list-style-type: none"> ● 任意攻击行为联动封锁 <p>对任意具有攻击特征的 IP 执行访问封锁，最大化业务和用户的安全防御能力。</p> <p>注意：开启联动封锁可有效阻断攻击者的后续攻击力，同时当业务系统代码不规范导致误判发生时，可能会引起业务无法访</p>

		问。
17	请求检测	检测 http/https 的请求 body 大小，最大支持 10M。
18	响应检测	检测 http/https 的相应 body 大小，最大支持 10M。
19	真实客户端 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，请在此填写代理头部字段和真实源 IP 的层数，用于识别真实的源 IP 进行日志记录和封锁；同时请关闭中低频 WEB 口令爆破防护，以防止误封锁代理 IP。
20	代理服务器 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，在此填写 CDN IP 或代理 IP，用于进行日志记录和联动封锁。

基础信息

* 站点名称

* 防护域名

* 服务类型 http https

* SSL策略

* 监听端口

输入单个端口或端口范围（如：80-88）后，按Enter键添加。最多可以添加16个

备注

请求信息

* 负载均衡算法 加权最小连接 源地址哈希 轮询

* 转发服务器 :

启用健康检查 [设置](#)

* 保持连接方式 短连接 长连接

默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接

会话保持 启用会话保持

* X-Forwarded-For

头部改写

头部改写

<input type="checkbox"/>	类型	动作	参数名	参数值	操作
暂无数据					

防护方式

* BOT防护策略

* WEB防护策略 展开详情

* 检测动作 检测后放行 检测后拦截

联动封锁 启用联动封锁

* 请求检测 请求检测body大小 KB

响应检测 启用响应检测

响应检测body大小 KB

真实客户端IP

<input type="checkbox"/>	头部字段	IP层数	操作
暂无数据			

代理服务器IP

步骤6. 配置完成后，点击<确定>即可完成配置。

新增	启用	禁用	删除	全部健康状态	全部WEB防护策略	全部BOT防护策略	站点名称/域名/监听端口	序号	健康状态	站点名称	防护域名	服务器类型	监听端口	WEB防护策略	BOT防护策略	启用/禁用	操作
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					1	正常	门户网站	a.sangfor.com	https	443	WEB防护策略	暂不使用BOT策略	<input checked="" type="checkbox"/>	编辑 复制 删除

步骤7. 若站点使用域名，则需要域名的解析修改成云WAF宿主机（单台设备部署）/云WAF检测节点（分离式设备部署）的地址。

修改记录 X

记录类型: A- 将域名指向一个IPV4地址 v

主机记录: 1.2.3.4.5.6 .dns-example.com ?

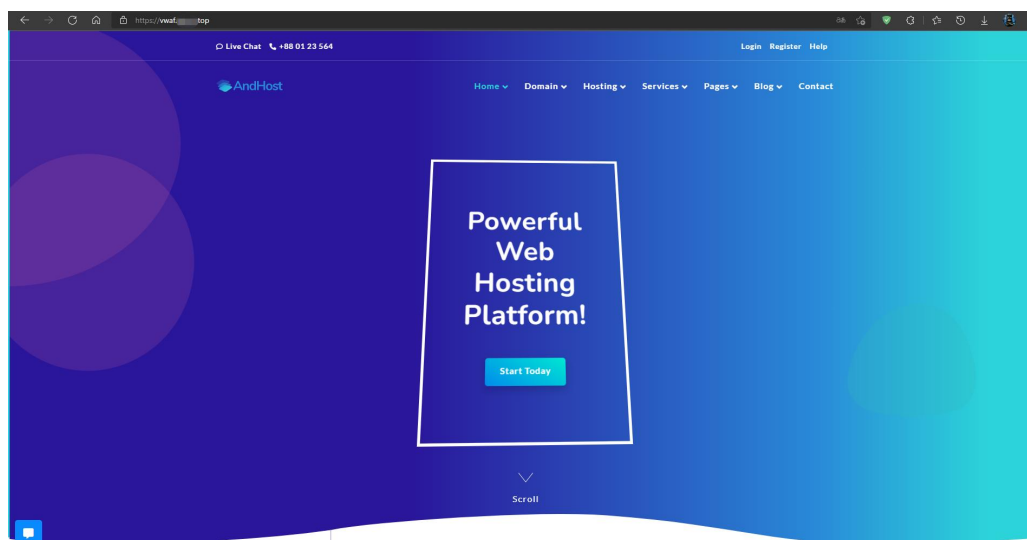
解析线路: 默认 - 必填! 未匹配到智能解析线路时, 返回【默认】线路... ?

* 记录值: 5.5.5.5

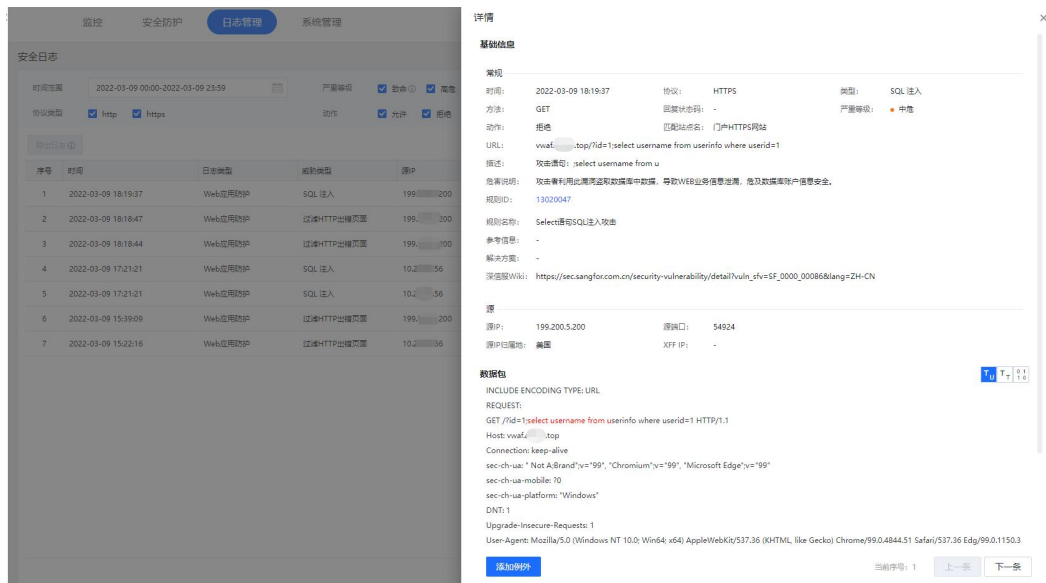
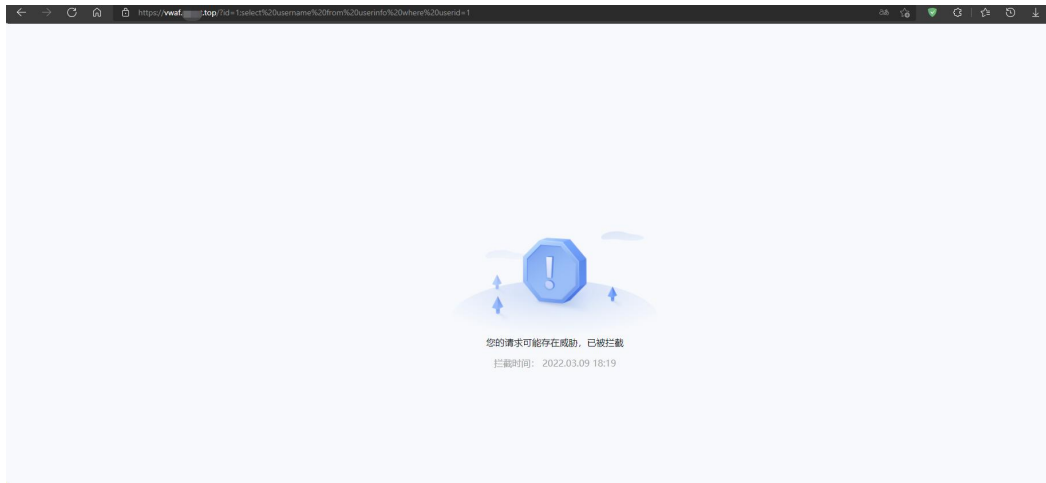
* TTL: 10分钟 v

4.1.2.4. 效果预览

使用浏览器访问站点，可以成功访问到配置的https服务器站点。



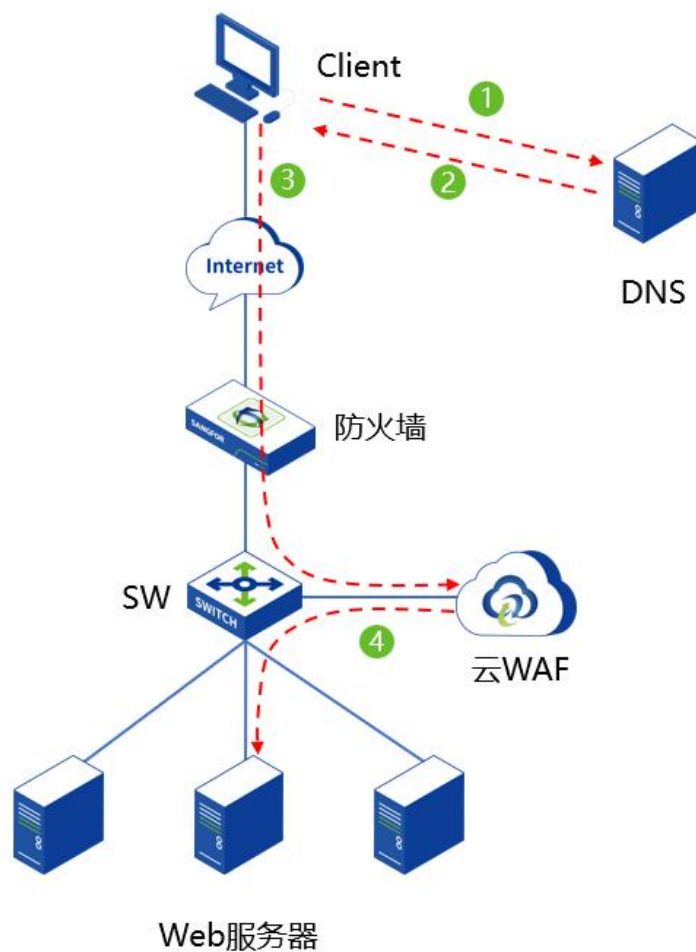
模拟进行攻击，成功拦截，并可以查询到安全日志。



4.1.3. HTTPS 站点防护配置案例_https 卸载

4.1.3.1. 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。



4.1.3.2. 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。

4.1.3.3. 配置步骤

步骤1. 在设备[安全防护/策略管理/WEB防护策略]中创建Web服务器的WEB防护策略，也可以直接复用默认策略模板。

安全防护 1 节点管理 日志管理 系统管理

WEB防护策略

新增 4 删除 高级设置

序号	策略名称	描述
1	默认策略_业务保护场景	建议在日常运营业务保护场景下使用，选取最准确的规则对命中攻击进行拦截，其余规则命中后仅
2	默认策略_非代理访问场景	建议在非代理场景下使用，在业务保护安全防护基础上，提供漏洞扫描能力，针对恶意的漏洞扫描

*策略名称 WEB防护策略

策略描述 请输入策略描述（选填）

防护配置

解析配置 XML解析

云端威胁情报 云端黑客IP防护

协议保护

HTTP应用隐藏 文件上传过滤 URL防护 HTTP异常检测 参数防护

CSRF防护 受限URL防护 口令防护 漏洞防扫描 CC攻击防护

漏洞保护

SQL注入	信息泄露攻击
XSS攻击	WEB整站系统漏洞
网站扫描	WEBSHELL后门通信
WEBSHELL	自定义规则
系统命令注入	WEB漏洞攻击
文件包含攻击	PHP代码注入防护
目录遍历攻击	JAVA代码注入防护
XXE攻击防护	后门扫描防护

步骤2. 在设备[安全防护/SSL策略/证书管理]中点击<新增>，导入SSL证书。

安全防护 1 节点管理 日志管理 系统管理

SSL策略管理 证书管理 3

新增 4 删除

序号	名称	签发时间	过期时间
1	默认证书	2021年10月6日 16:42:44	2031年10月4日 16:42:44

新增服务器证书 ×

*名称

描述

*颁发类型 导入证书文件 导入一对公私钥

*选择证书文件

密码

步骤3. 在设备[安全防护/SSL策略/SSL策略管理]中点击<新增>，添加SSL策略，选择导入的服务器证书，及启用的SSL协议和加密算法。



新增SSL策略 ×

*名称

描述

*服务器证书


*启用协议 TLS1.0 TLS1.1 TLS1.2 TLS1.3

*加密算法

已选 (18 / 18) ↑ ↓

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

待选 (0) 搜索关键字 🔍



暂无数据

步骤4. 在设备[安全防护/站点防护]中创建站点防护。



步骤5. 创建需要防护地址的相关参数。

序号	参数	说明
01	站点名称	配置进行代理防护的 Web 站点的策略名称。
02	防护域名	<p>需要防护的站点域名，支持 IP 地址和域名两种形式。</p> <ul style="list-style-type: none"> ● 填写 IP 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是 IP 地址，有内网使用私有 IP 访问需求，则填写云 WAF 宿主机 IP 地址；有互联网访问需求，则填写云 WAF 宿主机 IP 映射后的公网 IP 地址；若既有私有 IP 地址访问需求，也有公网 IP 地址访问需求，则均需填写。 ● 填写域名 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的

		防护域名若是域名，则域名的 DNS 解析需要解析成云 WAF 宿主机的 IP 地址或 NAT 映射后的地址。
03	服务类型	云 WAF 支持对 http 和 https 协议进行反向代理和安全防护。
04	监听端口	云 WAF 进行反向代理所监听的端口。 支持单个端口或端口范围（如：80-88）后，最多可以添加 16 个。
05	备注	对此防护策略进行备注描述，可留空。
06	负载调度算法	云 WAF 反向代理支持负载均衡算法调度，分别有[加权最小连接]、[源地址哈希]、[轮询]三种。 <ul style="list-style-type: none"> ● 加权最少连接 表示选择（连接数/权重）最小的节点。 ● 源地址哈希 根据源 IP 经过哈希运算得到哈希值，使不同的源 IP 尽可能平均调度节点池中各个节点，相同源 IP 的访问调度到同一个节点。 ● 轮询 表示交替返回有效的节点。
07	转发服务器	云 WAF 反向代理的真实服务器的地址。
08	启用健康检查	对转发服务器中的节点进行服务状态检查，支持 http/https/tcp 的检查方式，并且可以自定义检查的阈值。 注意：https 仅支持 SSLv3 协议，使用其他协议如 TLS1.2、TLS1.3 建议使用 tcp 的健康检查。
09	保持连接方式	<ul style="list-style-type: none"> ● 短连接 浏览器和服务器每进行一次 HTTP 操作，就建立一次连接，但任务结束就中断连接。在 HTTP/1.0 中，默认使用的是短连接。 ● 长连接 浏览器和服务器进行一次 HTTP 操作后，浏览器和服务器之间用于传输 HTTP 数据的 TCP 连接不会关闭，如果客户端再次访问这个服务器上的网页，会继续使用这一条已经建立的连接。从 HTTP/1.1 起，默认使用长连接。 云 WAF 默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接。
10	会话保持	会话保持是基于 Cookie 的会话保持方式，该方式匹配 HTTP 请求中的 Cookie 字段，通过不同 Cookie 区分不同客户端，可以将所有携带相同 Cookie 的 HTTP 流量转发到同一个转发服务器上面。并且可自定义设置会话保持时间，0 表示浏览器关闭时 cookie 失效，最大 24 小时。
11	X-Forwarded-For	X-Forwarded-For 实现了云 WAF 到服务器之间的客户端真实地址透传，后端服务器识别 X-Forwarded-For 字段可以知道访问客户端的真实 IP 地址。 <ul style="list-style-type: none"> ● 在末尾追加上一跳的 IP 地址 在 HTTP 头部追加插入 X-Forwarded-For 字段，为上一跳的 IP 地址。 ● 原封不动 不插入 X-Forwarded-For 字段。 ● 用上一跳的 IP 地址覆盖原有内容 在 HTTP 头部插入 X-Forwarded-For 字段，为上一跳的 IP 地

		址。若 HTTP 头部存在 X-Forwarded-For 字段，则用上一跳的 IP 地址覆盖原有内容。
12	头部改写	可以对 HTTP 的请求头、相应头进行添加或是隐藏相关参数。
13	WEB 防护策略	调用创建的 WEB 防护策略，若选择暂不使用 WEB 防护策略，则只对站点进行反向代理，不进行 WEB 安全防护。
14	BOT 防护策略	调用创建的 BOT 防护策略，若选择暂不使用 BOT 防护策略，则只对站点进行反向代理，不进行 BOT 安全防护。
15	检测动作	检查动作分为“检测后放行”、“检测后拦截”两种。
16	联动封锁	<p>联动封锁分为“高危行为联动封锁”、“任意攻击行为联动封锁”两种。</p> <ul style="list-style-type: none"> ● 高危行为联动封锁 <p>仅封锁具有高危行为特征的 IP，优先保证用户流畅上网、业务稳定的提供服务。</p> <ul style="list-style-type: none"> ● 任意攻击行为联动封锁 <p>对任意具有攻击特征的 IP 执行访问封锁，最大化业务和用户的安全防御能力。</p> <p>注意：开启联动封锁可有效阻断攻击者的后续攻击力，同时当业务系统代码不规范导致误判发生时，可能会引起业务无法访问。</p>
17	请求检测	检测 http/https 的请求 body 大小，最大支持 10M。
18	响应检测	检测 http/https 的相应 body 大小，最大支持 10M。
19	真实客户端 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，请在此填写代理头部字段和真实源 IP 的层数，用于识别真实的源 IP 进行日志记录和封锁；同时请关闭中低频 WEB 口令爆破防护，以防止误封锁代理 IP。
20	代理服务器 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，在此填写 CDN IP 或代理 IP，用于进行日志记录和联动封锁。

基础信息

* 站点名称

* 防护域名

* 服务类型 http https

* SSL策略

* 监听端口
输入单个端口或端口范围（如：80-88）后，按Enter键添加。最多可以添加16个

备注

请求信息

* 负载调度算法 加权最小连接 源地址哈希 轮询

* 转发服务器 :

启用健康检查 [设置](#)

* 保持连接方式 短连接 长连接
默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接

会话保持 启用会话保持

* X-Forwarded-For

头部改写

头部改写

<input type="button" value="新增"/> <input type="button" value="删除"/>					
<input type="checkbox"/>	类型	动作	参数名	参数值	操作
暂无数据					

防护方式

*BOT防护策略

*WEB防护策略

*检测动作 检测后放行 检测后拦截

联动封锁 启用联动封锁 ?

*请求检测 请求检测body大小 KB

响应检测 启用响应检测

响应检测body大小 KB

真实客户端IP ?

<input type="button" value="新增"/> <input type="button" value="删除"/>			
<input type="checkbox"/>	头部字段	IP层数	操作
暂无数据			

代理服务器IP ?

步骤6. 配置完成后，点击<确定>即可完成配置。

<input type="button" value="新增"/>	<input type="button" value="应用"/>	<input type="button" value="禁用"/>	<input type="button" value="删除"/>	全部健康状态	全部WEB防护策略	全部BOT防护策略	站点名称/域名/应用端口	<input type="text"/>	<input type="button" value="C"/>	
<input type="checkbox"/>	序号	健康状态	站点名称	防护域名	服务类型	监听端口	WEB防护策略	BOT防护策略	启用/禁用	操作
<input type="checkbox"/>	1	正常	门户网站	asangfor.com	https	443	WEB防护策略	暂不使用BOT策略	<input checked="" type="checkbox"/>	<input type="button" value="编辑"/> <input type="button" value="复制"/> <input type="button" value="删除"/>

步骤7. 若站点使用域名，则需要域名的解析修改成云WAF宿主机（单台设备部署）/云WAF检测节点（分离式设备部署）的地址。

修改记录 X

记录类型: A- 将域名指向一个IPV4地址 v

主机记录: 1.2.3.4.5.6 .dns-example.com ?

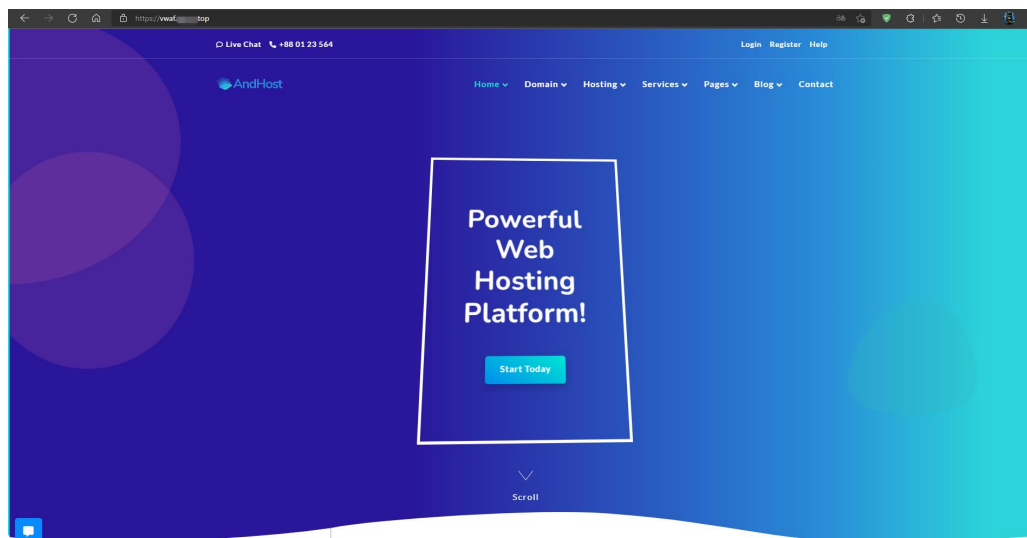
解析线路: 默认 - 必填! 未匹配到智能解析线路时, 返回【默认】线路... ?

* 记录值: 5.5.5.5

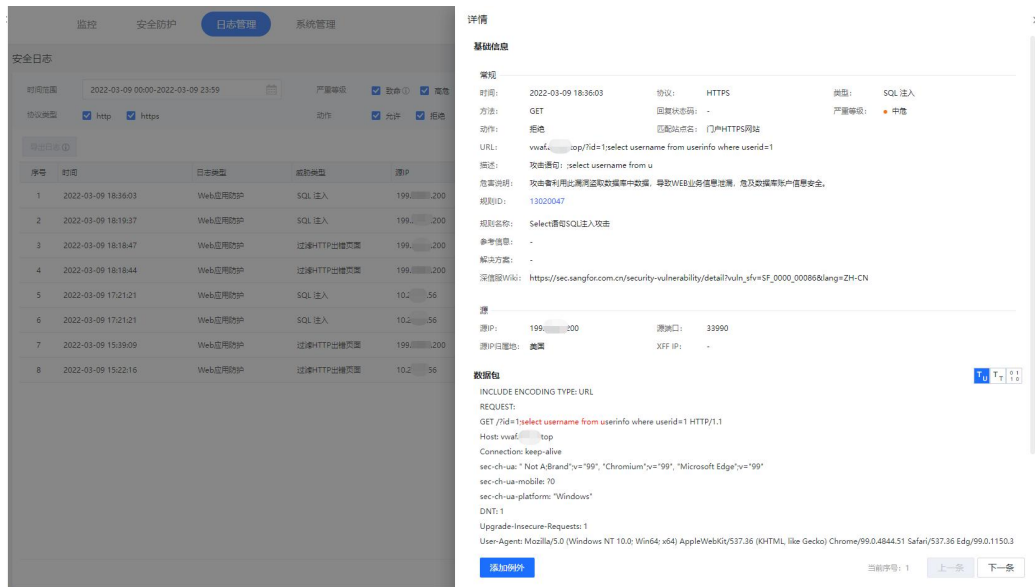
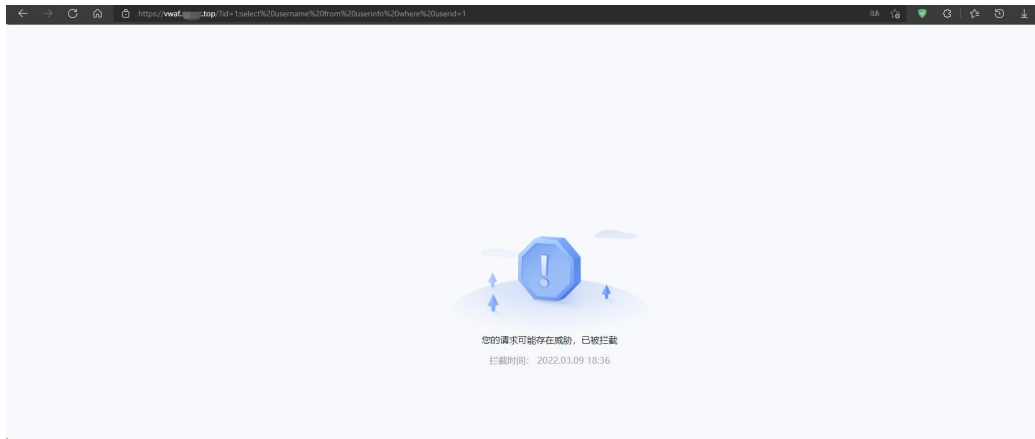
* TTL: 10 分钟 v

4.1.3.4. 效果预览

使用浏览器访问站点，可以成功使用https协议访问http服务器站点。



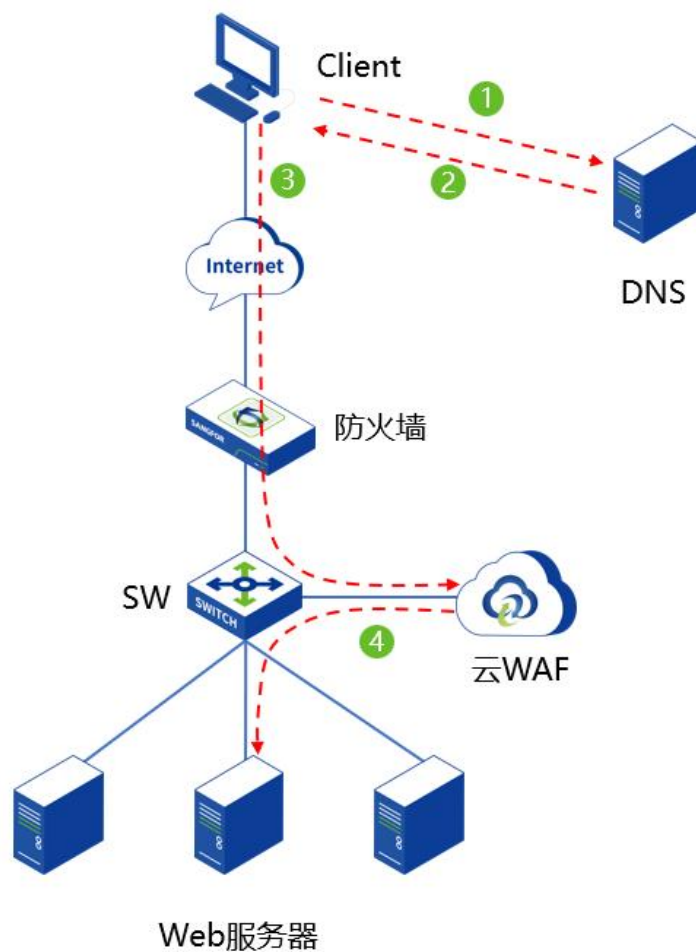
模拟进行攻击，成功拦截，并可以查询到安全日志。



4.1.4. 一个 HTTP 端口负载多个 HTTP 站点防护配置案例

4.1.4.1. 需求背景

客户业务中存在3台承载不同业务的HTTP服务器，对外只发布TCP 80 端口。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。



4.1.4.2. 需求分析

一个端口同时负载不同的业务，需要使用不同的地址或域名区分，服务器A的业务使用 a.sangfor.com，服务器B的业务使用 b.sangfor.com，服务器C的业务使用 c.sangfor.com来进行调度，并进行安全防护。

4.1.4.3. 配置步骤

步骤1. 在设备[安全防护/策略管理/WEB防护策略]中创建Web服务器的WEB防护策略，也可以直接复用默认策略模板。



深信服WAF 监控 **安全防护** 1 节点管理 日志管理 系统管理

安全防护 < | 策略管理 > | WEB防护策略 > | BOT防护策略 | 例外策略 | 安全防护规则库 > | SSL策略 | 黑白名单 > | 云端黑名单防护

WEB防护策略

新增 4 删除 高级设置

序号	策略名称	描述
1	默认策略_业务保护场景	建议在日常运营业务保护场景下使用，选取最准确的规则对命中攻击进行拦截，其余规则命中后仅
2	默认策略_非代理访问场景	建议在非代理场景下使用，在业务保护安全防护基础上，提供漏洞扫描能力，针对恶意的漏洞扫描

*策略名称: WEB防护策略

策略描述: 请输入策略描述 (选填)

防护配置

解析配置 XML解析

云端威胁情报 云端黑客IP防护

协议保护: HTTP应用隐藏, 文件上传过滤, URL防护, HTTP异常检测, 参数防护

CSRF防护, 受限URL防护, 口令防护, 漏洞防扫描, CC攻击防护

漏洞保护

SQL注入	✓	信息泄露攻击	✓
XSS攻击	✓	WEB整站系统漏洞	✓
网站扫描	✓	WEBSHELL后门通信	✓
WEBSHELL	✓	自定义规则	✓
系统命令注入	✓	WEB漏洞攻击	✓
文件包含攻击	✓	PHP代码注入防护	✓
目录遍历攻击	✓	JAVA代码注入防护	✓
XXE攻击防护	✓	后门扫描防护	✓

步骤2. 在设备[安全防护/站点防护]中创建a.sangfor.com站点防护。



步骤3. 创建需要防护地址的相关参数。

序号	参数	说明
01	站点名称	配置进行代理防护的 Web 站点的策略名称。
02	防护域名	需要防护的站点域名，支持 IP 地址和域名两种形式。 <ul style="list-style-type: none"> ● 填写 IP 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是 IP 地址，有内网使用私有 IP 访问需求，则填写云 WAF 宿主机 IP 地址；有互联网访问需求，则填写云 WAF 宿主机 IP 映射后的公网 IP 地址；若既有私有 IP 地址访问需求，也有公网 IP 地址访问需求，则均需填写。 ● 填写域名 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是域名，则域名的 DNS 解析需要解析成云 WAF 宿主机的 IP 地址或 NAT 映射后的地址。
03	服务类型	云 WAF 支持对 http 和 https 协议进行反向代理和安全防护。
04	监听端口	云 WAF 进行反向代理所监听的端口。 支持单个端口或端口范围（如：80-88）后，最多可以添加 16 个。
05	备注	对此防护策略进行备注描述，可留空。
06	负载调度算法	云 WAF 反向代理支持负载均衡算法调度，分别有[加权最小连接]、[源地址哈希]、[轮询]三种。 <ul style="list-style-type: none"> ● 加权最少连接 表示选择（连接数/权重）最小的节点。 ● 源地址哈希 根据源 IP 经过哈希运算得到哈希值，使不同的源 IP 尽可能平均调度节点池中各个节点，相同源 IP 的访问调度到同一个节点。 ● 轮询 表示交替返回有效的节点。
07	转发服务器	云 WAF 反向代理的真实服务器的地址。
08	启用健康检查	对转发服务器中的节点进行服务状态检查，支持 http/https/tcp 的检查方式，并且可以自定义检查的阈值。

09	保持连接方式	<ul style="list-style-type: none"> ● 短连接 浏览器和服务器每进行一次 HTTP 操作，就建立一次连接，但任务结束就中断连接。在 HTTP/1.0 中，默认使用的是短连接。 ● 长连接 浏览器和服务器进行一次 HTTP 操作后，浏览器和服务器之间用于传输 HTTP 数据的 TCP 连接不会关闭，如果客户端再次访问这个服务器上的网页，会继续使用这一条已经建立的连接。从 HTTP/1.1 起，默认使用长连接。 云 WAF 默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接。
10	会话保持	会话保持是基于 Cookie 的会话保持方式，该方式匹配 HTTP 请求中的 Cookie 字段，通过不同 Cookie 区分不同客户端，可以将所有携带相同 Cookie 的 HTTP 流量转发到同一个转发服务器上面。并且可自定义设置会话保持时间，0 表示浏览器关闭时 cookie 失效，最大 24 小时。
11	X-Forwarded-For	<p>X-Forwarded-For 实现了云 WAF 到服务器之间的客户端真实地址透传，后端服务器识别 X-Forwarded-For 字段可以知道访问客户端的真实 IP 地址。</p> <ul style="list-style-type: none"> ● 在末尾追加上一跳的 IP 地址 在 HTTP 头部追加插入 X-Forwarded-For 字段，为上一跳的 IP 地址。 ● 原封不动 不插入 X-Forwarded-For 字段。 ● 用上一跳的 IP 地址覆盖原有内容 在 HTTP 头部插入 X-Forwarded-For 字段，为上一跳的 IP 地址。若 HTTP 头部存在 X-Forwarded-For 字段，则用上一跳的 IP 地址覆盖原有内容。
12	头部改写	可以对 HTTP 的请求头、相应头进行添加或是隐藏相关参数。
13	WEB 防护策略	调用创建的 WEB 防护策略，若选择暂不使用 WEB 防护策略，则只对站点进行反向代理，不进行 WEB 安全防护。
14	BOT 防护策略	调用创建的 BOT 防护策略，若选择暂不使用 BOT 防护策略，则只对站点进行反向代理，不进行 BOT 安全防护。
15	检测动作	检查动作分为“检测后放行”、“检测后拦截”两种。
16	联动封锁	<p>联动封锁分为“高危行为联动封锁”、“任意攻击行为联动封锁”两种。</p> <ul style="list-style-type: none"> ● 高危行为联动封锁 仅封锁具有高危行为特征的 IP，优先保证用户流畅上网、业务稳定的提供服务。 ● 任意攻击行为联动封锁 对任意具有攻击特征的 IP 执行访问封锁，最大化业务和用户的安全防御能力。 <p>注意：开启联动封锁可有效阻断攻击者的后续攻击力，同时当业务系统代码不规范导致误判发生时，可能会引起业务无法访问。</p>
17	请求检测	检测 http/https 的请求 body 大小，最大支持 10M。
18	响应检测	检测 http/https 的相应 body 大小，最大支持 10M。

19	真实客户端 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，请在此填写代理头部字段和真实源 IP 的层数，用于识别真实的源 IP 进行日志记录和封锁；同时请关闭中低频 WEB 口令爆破防护，以防止误封锁代理 IP。
20	代理服务器 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，在此填写 CDN IP 或代理 IP，用于进行日志记录和联动封锁。

基础信息

* 站点名称

* 防护域名

* 服务类型 http https

* 监听端口 ×
 输入单个端口或端口范围（如：80-88）后，按Enter键添加。最多可以添加16个

备注

请求信息

* 负载均衡算法 加权最小连接 源地址哈希 轮询

* 转发服务器
 : ×
 : ×
 : ×

启用健康检查 [设置](#)

* 保持连接方式 短连接 长连接
 默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接

会话保持 启用会话保持

会话保持时间 小时

* X-Forwarded-For

头部改写

<input type="checkbox"/>	类型	动作	参数名	参数值	操作
暂无数据					

防护方式

* BOT防护策略

* WEB防护策略

* 检测动作 检测后放行 检测后拦截

联动封锁 启用联动封锁 ^①

* 请求检测 请求检测body大小 KB

响应检测 启用响应检测

响应检测body大小 KB

真实客户端IP ^①

<input type="checkbox"/>	头部字段	IP层数	操作
暂无数据			

代理服务器IP ^①

步骤4. 同理创建b.sangfor.com和c.sangfor.com的站点防护，防护域名和转发服务器配置成服务器B和服务器C的。

基础信息

* 站点名称

* 防护域名

* 服务类型 http https

* 监听端口
输入单个端口或端口范围 (如: 80-88) 后, 按Enter键添加。最多可以添加16个

备注

请求信息

* 负载调度算法 加权最小连接 源地址哈希 轮询

* 转发服务器 | . :

启用健康检查 [设置](#)

* 保持连接方式 短连接 长连接
默认使用长连接, 请确认转发服务器是否支持长连接, 若不支持, 即使设置为长连接, 也会使用短连接

会话保持 启用会话保持

会话保持时间

* X-Forwarded-For

头部改写

<input type="checkbox"/>	类型	动作	参数名	参数值	操作
<input type="button" value="新增"/>					<input type="button" value="删除"/>

头部改写

<input type="checkbox"/>	类型	动作	参数名	参数值	操作
暂无数据					

防护方式

* BOT防护策略

* WEB防护策略

* 检测动作 检测后放行 检测后拦截

联动封锁 启用联动封锁 ^①

* 请求检测 请求检测body大小 KB

响应检测 启用响应检测

响应检测body大小 KB

真实客户端IP ^①

<input type="checkbox"/>	头部字段	IP层数	操作
暂无数据			

代理服务器IP ^①

步骤5. 将域名的解析修改成云WAF宿主机（单台设备部署）/云WAF检测节点（分离式设备部署）的地址。

修改记录

X

记录类型:

主机记录: .dns-example.com ^①

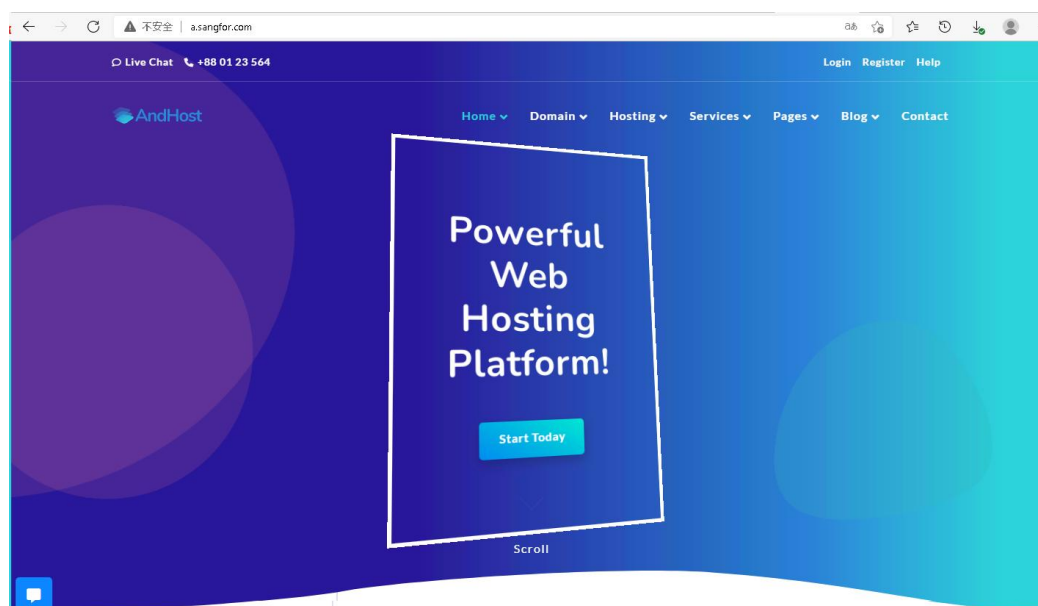
解析线路: ^①

* 记录值:

* TTL:

4.1.4.4. 效果预览

使用浏览器访问<http://a.sangfor.com>可以成功访问A站点。



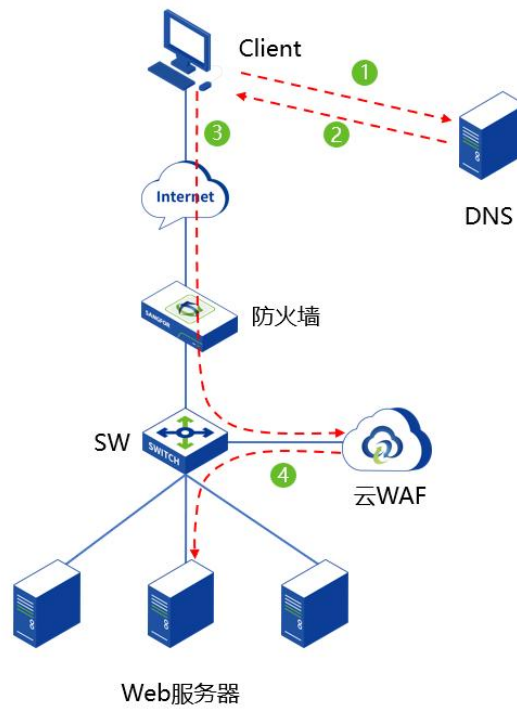
使用浏览器访问<http://b.sangfor.com>可以成功访问B站点。



4.1.5. 站点策略 BOT 防护配置案例

4.1.5.1. 需求背景

某企业使用云WAF做WEB服务器的防护，用户要求对WEB的自动化BOT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。

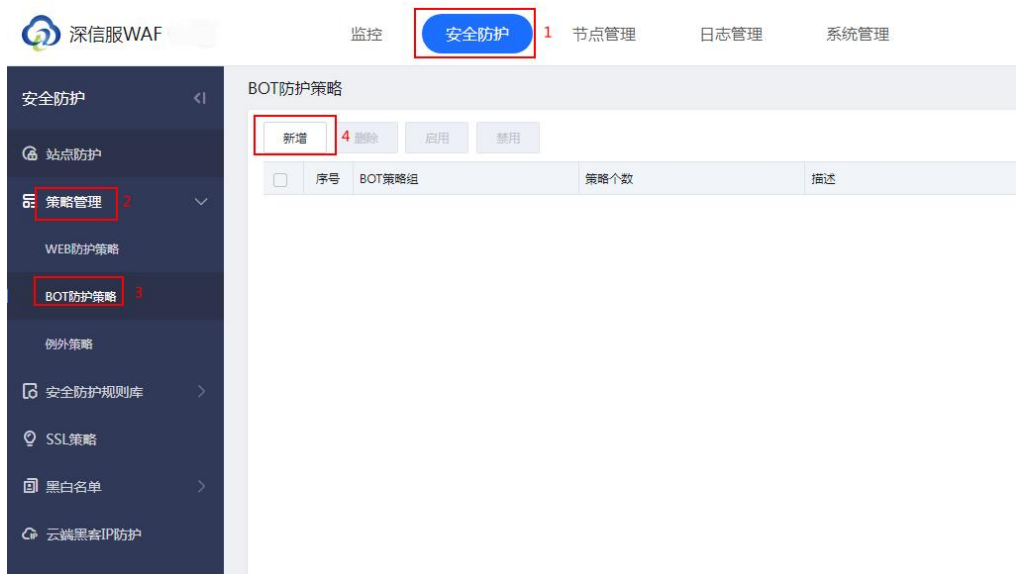


4.1.5.2. 需求分析

针对这些需求，需要使用BOT防护策略功能，来对自动化攻击流量进行检测发现存在的攻击行为。

4.1.5.3. 配置步骤

步骤1. 在设备[安全防护/策略管理/BOT防护策略]中创建Web服务器的BOT防护策略。





步骤2. 在设备[安全防护/站点防护]中创建站点防护。



步骤3. 创建需要防护地址的相关参数。

序号	参数	说明
01	站点名称	配置进行代理防护的 Web 站点的策略名称。
02	防护域名	需要防护的站点域名，支持 IP 地址和域名两种形式。 <ul style="list-style-type: none"> ● 填写 IP 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是 IP 地址，有内网使用私有 IP 访问需求，则填写云 WAF 宿主机 IP 地址；有互联网访问需求，则填写云 WAF 宿主机 IP 映射后的公网 IP 地址；若既有私有 IP 地址访问需求，也有公网 IP 地址访问需求，则均需填写。 ● 填写域名 云 WAF 会对需要防护的 Web 站点进行反向代理，此处填写的防护域名若是域名，则域名的 DNS 解析需要解析成云 WAF 宿主机的 IP 地址或 NAT 映射后的地址。
03	服务类型	云 WAF 支持对 http 和 https 协议进行反向代理和安全防护。
04	监听端口	云 WAF 进行反向代理所监听的端口。 支持单个端口或端口范围（如：80-88）后，最多可以添加 16 个。
05	备注	对此防护策略进行备注描述，可留空。

06	负载调度算法	<p>云 WAF 反向代理支持负载均衡算法调度，分别有[加权最小连接]、[源地址哈希]、[轮询]三种。</p> <ul style="list-style-type: none"> ● 加权最少连接 表示选择（连接数/权重）最小的节点。 ● 源地址哈希 根据源 IP 经过哈希运算得到哈希值，使不同的源 IP 尽可能平均调度节点池中各个节点，相同源 IP 的访问调度到同一个节点。 ● 轮询 表示交替返回有效的节点。
07	转发服务器	云 WAF 反向代理的真实服务器的地址。
08	启用健康检查	对转发服务器中的节点进行服务状态检查，支持 http/https/tcp 的检查方式，并且可以自定义检查的阈值。
09	保持连接方式	<ul style="list-style-type: none"> ● 短连接 浏览器和服务端每进行一次 HTTP 操作，就建立一次连接，但任务结束就中断连接。在 HTTP/1.0 中，默认使用的是短连接。 ● 长连接 浏览器和服务端进行一次 HTTP 操作后，浏览器和服务端之间用于传输 HTTP 数据的 TCP 连接不会关闭，如果客户端再次访问这个服务器上的网页，会继续使用这一条已经建立的连接。从 HTTP/1.1 起，默认使用长连接。 云 WAF 默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接。
10	会话保持	会话保持是基于 Cookie 的会话保持方式，该方式匹配 HTTP 请求中的 Cookie 字段，通过不同 Cookie 区分不同客户端，可以将所有携带相同 Cookie 的 HTTP 流量转发到同一个转发服务器上面。并且可自定义设置会话保持时间，0 表示浏览器关闭时 cookie 失效，最大 24 小时。
11	X-Forwarded-For	<p>X-Forwarded-For 实现了云 WAF 到服务器之间的客户端真实地址透传，后端服务器识别 X-Forwarded-For 字段可以知道访问客户端的真实 IP 地址。</p> <ul style="list-style-type: none"> ● 在末尾追加上一跳的 IP 地址 在 HTTP 头部追加插入 X-Forwarded-For 字段，为上一跳的 IP 地址。 ● 原封不动 不插入 X-Forwarded-For 字段。 ● 用上一跳的 IP 地址覆盖原有内容 在 HTTP 头部插入 X-Forwarded-For 字段，为上一跳的 IP 地址。若 HTTP 头部存在 X-Forwarded-For 字段，则用上一跳的 IP 地址覆盖原有内容。
12	头部改写	可以对 HTTP 的请求头、相应头进行添加或是隐藏相关参数。
13	WEB 防护策略	调用创建的 WEB 防护策略，若选择暂不使用 WEB 防护策略，则只对站点进行反向代理，不进行 WEB 安全防护。
14	BOT 防护策略	调用创建的 BOT 防护策略，若选择暂不使用 BOT 防护策略，则只对站点进行反向代理，不进行 BOT 安全防护。
15	检测动作	检查动作分为“检测后放行”、“检测后拦截”两种。
16	联动封锁	联动封锁分为“高危行为联动封锁”、“任意攻击行为联动封

		<p>锁”两种。</p> <ul style="list-style-type: none"> ● 高危行为联动封锁 <p>仅封锁具有高危行为特征的 IP，优先保证用户流畅上网、业务稳定的提供服务。</p> <ul style="list-style-type: none"> ● 任意攻击行为联动封锁 <p>对任意具有攻击特征的 IP 执行访问封锁，最大化业务和用户的安全防御能力。</p> <p>注意：开启联动封锁可有效阻断攻击者的后续攻击力，同时当业务系统代码不规范导致误判发生时，可能会引起业务无法访问。</p>
17	请求检测	检测 http/https 的请求 body 大小，最大支持 10M。
18	响应检测	检测 http/https 的相应 body 大小，最大支持 10M。
19	真实客户端 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，请在此填写代理头部字段和真实源 IP 的层数，用于识别真实的源 IP 进行日志记录和封锁；同时请关闭中低频 WEB 口令爆破防护，以防止误封锁代理 IP。
20	代理服务器 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，在此填写 CDN IP 或代理 IP，用于进行日志记录和联动封锁。

基础信息

* 站点名称

* 防护域名

* 服务类型 http https

* 监听端口 输入单个端口或端口范围（如：80-88）后，按Enter键添加。最多可以添加16个

备注

请求信息

* 负载均衡算法 加权最小连接 源地址哈希 轮询

* 转发服务器 :

启用健康检查 [设置](#)

* 保持连接方式 短连接 长连接

默认使用长连接，请确认转发服务器是否支持长连接，若不支持，即使设置为长连接，也会使用短连接

会话保持 启用会话保持

会话保持时间 ①

* X-Forwarded-For

头部改写

<input type="checkbox"/>	类型	动作	参数名	参数值	操作
暂无数据					

防护方式

* BOT防护策略:

* WEB防护策略: 展开详情

* 请求检测: 请求检测body大小 KB

响应检测: 启用响应检测

响应检测body大小 KB

真实客户端IP ?

<input type="checkbox"/>	头部字段	IP层数	操作
暂无数据			

代理服务器IP ?

请填写受信任的真实CDN IP或代理IP, 每行一条数据

步骤4. 配置完成后, 点击<确定>即可完成配置。

新增	启用	禁用	删除	全部健康状态	全部WEB防护策略	全部BOT防护策略	站点名称/域名/监听端口
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				10.90.8.93

步骤5. 若站点使用域名, 则需要域名的解析修改成云WAF宿主机(单台设备部署)/云WAF检测节点(分离式设备部署)的地址。

修改记录 X

记录类型:

主机记录: ?

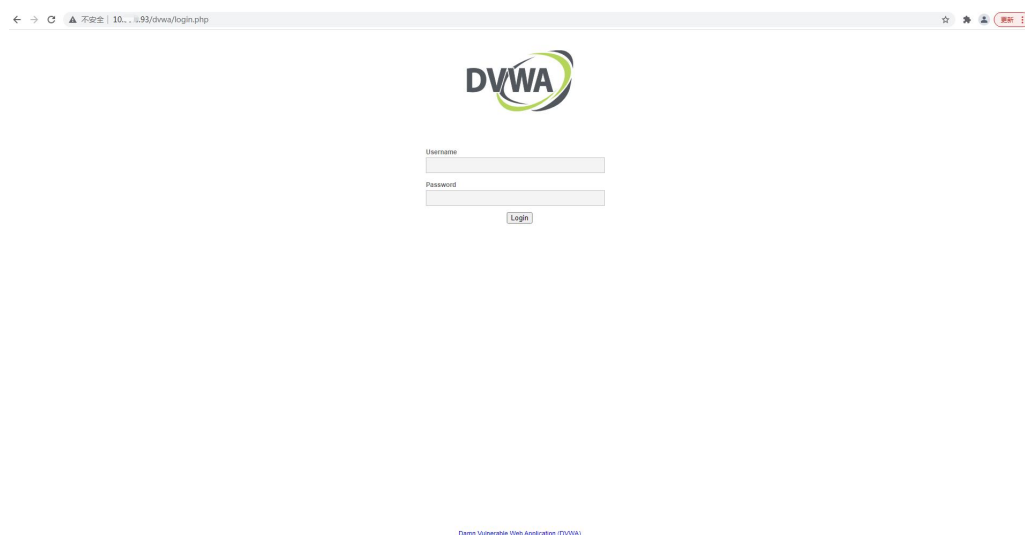
解析线路: ?

* 记录值:

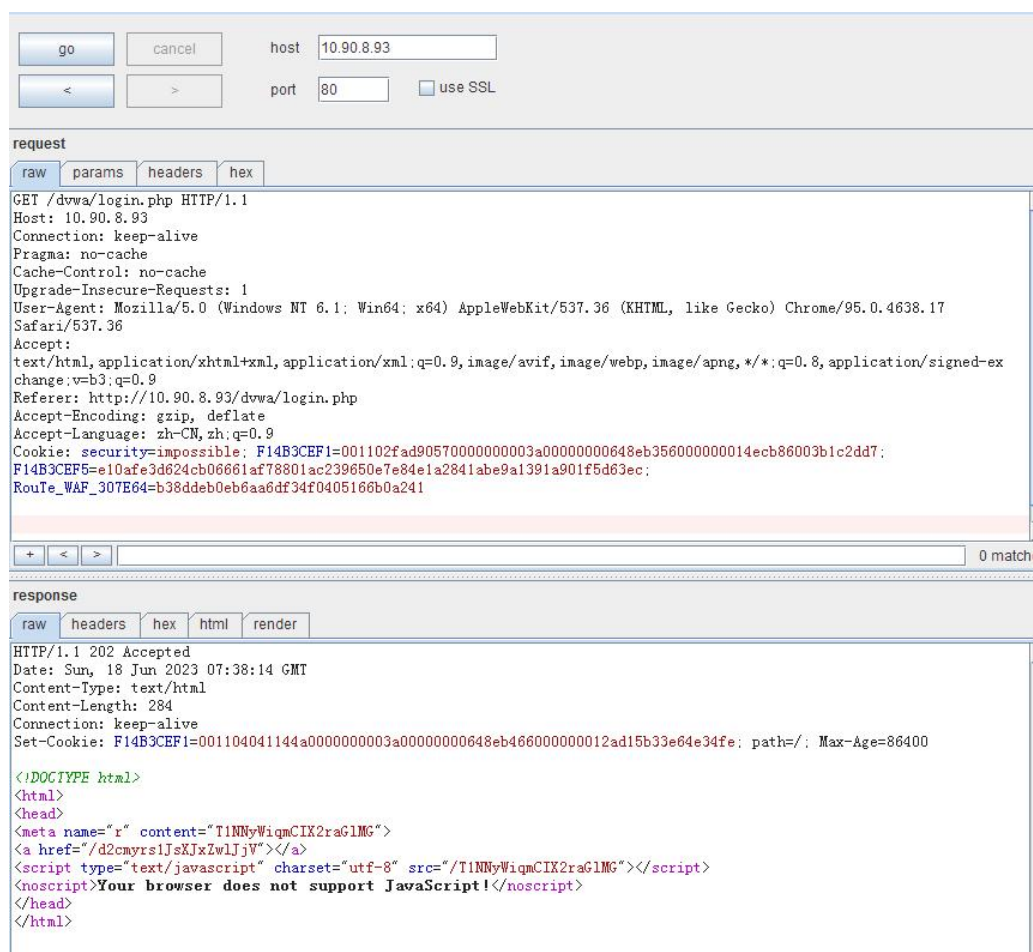
* TTL:

4.1.5.4. 效果预览

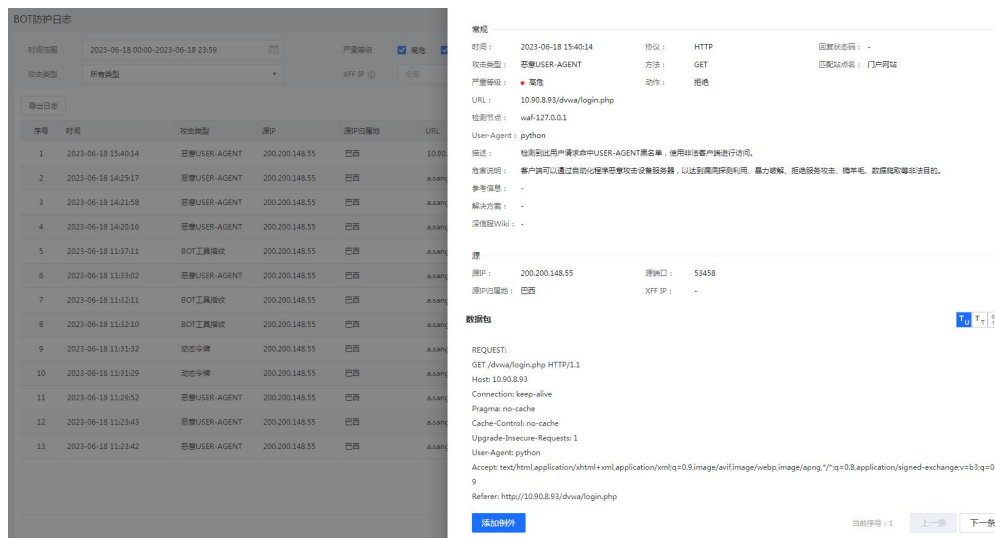
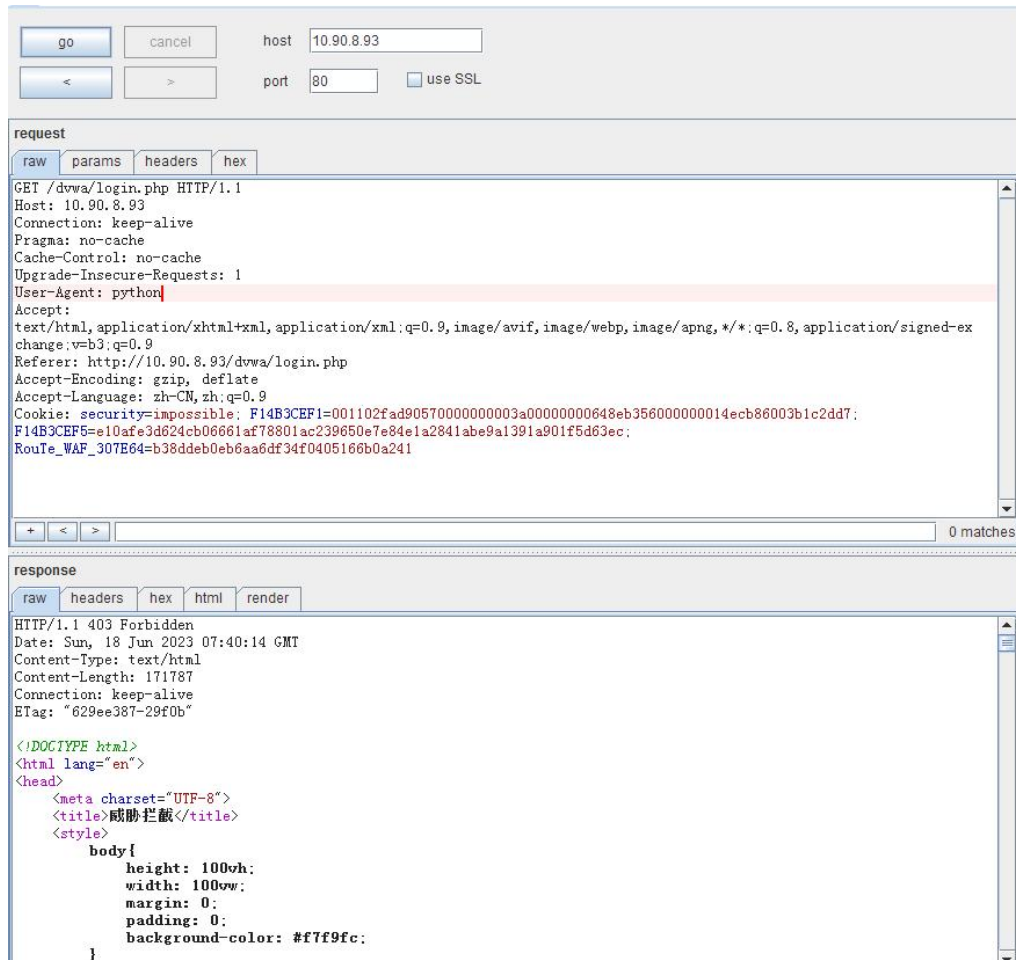
使用浏览器访问配置的BOT防护页面，可以成功访问。



使用自动化工具（如Burpsuit）访问配置的BOT防护页面，访问失败



使用自动化工具（如Burpsuit）User-Agent字段携带非浏览器特征信息，访问配置的BOT防护页面，成功拦截，并可以查询到安全日志

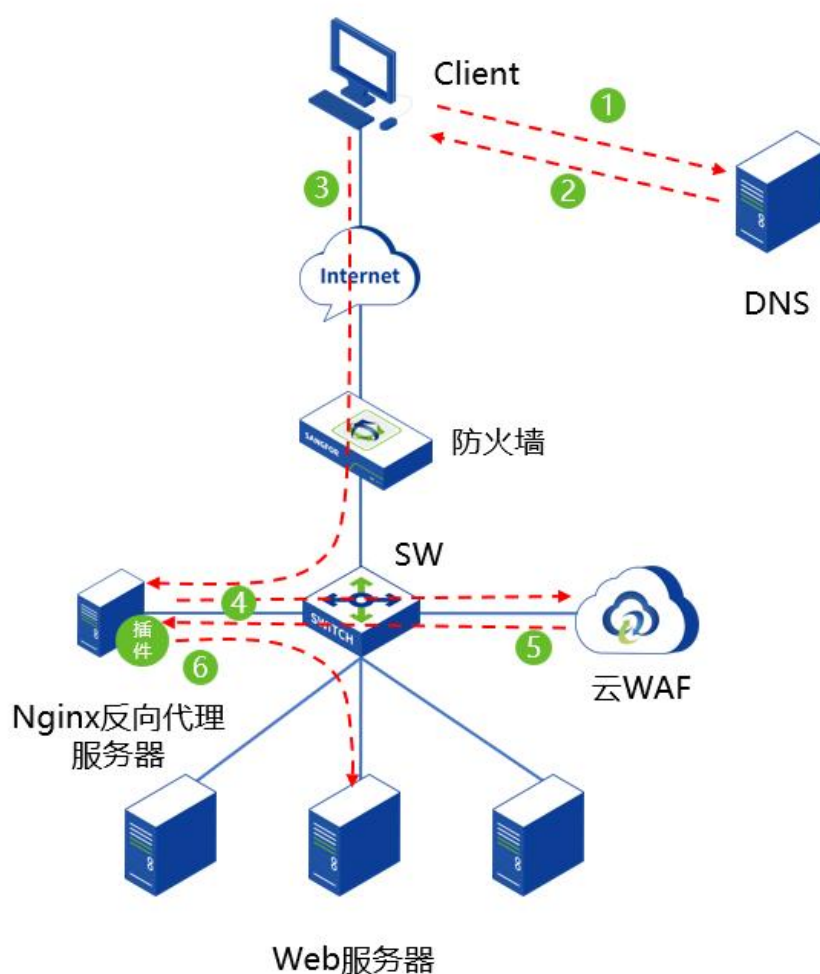


4.2. 插件模式

4.2.1. HTTP/HTTPS 站点防护配置案例

4.2.1.1. 需求背景

客户业务中存在3台HTTP服务器，前置有Nginx服务器对HTTP服务器进行业务负载，但业务服务器经常遭受来自互联网的扫描攻击，给服务器带来较大风险，且不想对网络进行较大的调整。



4.2.1.2. 需求分析

WEB服务器遭遇到互联网攻击，需要使用云WAF来防护WEB服务器的安全。客户具备Nginx服务器进行负载，且不想对网络进行较大的调整，云WAF插件可以部署在Nginx服务器上，将Nginx服务器的流量引流到云WAF的检测节点进行安全检测后，

再转发到各个服务器上。

4.2.1.3. 配置步骤

步骤1. 在设备[安全防护/策略管理/WEB防护策略]中创建Web服务器的WEB防护策略，也可以直接复用默认策略模板。

The screenshot displays the 'WEB防护策略' (Web Protection Policy) configuration page in the深信服WAF management console. The interface includes a sidebar with navigation options like '安全防护', '策略管理', and 'WEB防护策略'. The main area shows a table of existing policies and a configuration form for a new policy named 'WEB防护策略'.

策略管理

序号	策略名称	描述
1	默认策略_业务保护场景	建议在日常运维业务保护场景下使用，选取最准确的规则对命中攻击进行拦截，其余规则命中后仅
2	默认策略_非代理访问场景	建议在非代理场景下使用，在业务保护安全防护基础上，提供漏洞扫描能力，针对恶意的漏洞扫描

策略配置

*策略名称: WEB防护策略

策略描述: 请输入策略描述 (选填)

防护配置

解析配置: XML解析

云端威胁情报: 云端黑客IP防护

协议保护: HTTP应用隐藏, 文件上传过滤, URL防护, HTTP异常检测, 参数防护

CSRF防护, 受限URL防护, 口令防护, 漏洞防扫描, CC攻击防护

漏洞保护

SQL注入	信息泄露攻击
XSS攻击	WEB整站系统漏洞
网站扫描	WEBSHELL后门通信
WEBSHELL	自定义规则
系统命令注入	WEB漏洞攻击
文件包含攻击	PHP代码注入防护
目录遍历攻击	JAVA代码注入防护
XXE攻击防护	后门扫描防护

步骤2. 在设备[安全防护/站点防护]中创建站点防护。



步骤3. 创建需要防护地址的相关参数。

序号	参数	说明
01	站点名称	配置进行代理防护的 Web 站点的策略名称。
02	防护域名	需要防护的站点域名，支持 IP 地址和域名两种形式。
03	监听端口	填写站点所用的端口。 支持单个端口或端口范围（如：80-88）后，最多可以添加 16 个。
04	备注	对此防护策略进行备注描述，可留空。
05	WEB 防护策略	调用创建的 WEB 防护策略，若选择暂不使用 WEB 防护策略，则只对站点进行转发，不进行 WEB 安全防护。
06	BOT 防护策略	调用创建的 BOT 防护策略，若选择暂不使用 BOT 防护策略，则只对站点进行转发，不进行 BOT 安全防护。
07	检测动作	检查动作分为“检测后放行”、“检测后拦截”两种。
08	联动封锁	联动封锁分为“高危行为联动封锁”、“任意攻击行为联动封锁”两种。 <ul style="list-style-type: none"> ● 高危行为联动封锁 仅封锁具有高危行为特征的 IP，优先保证用户流畅上网、业务稳定的提供服务。 ● 任意攻击行为联动封锁 对任意具有攻击特征的 IP 执行访问封锁，最大化业务和用户的安全防御能力。 注意：开启联动封锁可有效阻断攻击者的后续攻击力，同时当业务系统代码不规范导致误判发生时，可能会引起业务无法访问。
09	真实客户端 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，请在此填写代理头部字段和真实源 IP 的层数，用于识别真实的源 IP 进行日志记录和封锁；同时请关闭中低频 WEB 口令爆破防护，以防止误封锁代理 IP。
10	代理服务器 IP	如果访问经过 CDN，或网络环境中部署了代理设备或负载均衡设备，在此填写 CDN IP 或代理 IP，用于进行日志记录和联动封锁。

基础信息

* 站点名称

* 防护域名

* 监听端口

输入单个端口或端口范围（如：80-88）后，按Enter键添加。最多可以添加16个

备注

防护方式

* BOT防护策略

* WEB防护策略

* 检测动作 检测后放行 检测后拦截

联动封锁

真实客户端IP

<input type="checkbox"/>	头部字段	IP层数	操作
暂无数据			

代理服务IP

步骤4. 配置完成后，点击<确定>即可完成配置。

新增	应用	禁用	删除	全部WEB防护策略	全部BOT防护策略	站点名称/域名/监听端口	操作	
<input type="checkbox"/>	序号	站点名称	防护域名	监听端口	WEB防护策略	BOT防护策略	应用/禁用	操作
<input type="checkbox"/>	1	站点防护	10.243.3.67	80	WEB防护策略	暂不使用BOT策略	<input checked="" type="checkbox"/>	编辑 复制 删除

步骤5. 将对应版本的so插件和引流配置模板拷贝到nginx安装目录，修改nginx.conf的配置，将云WAF插件和引流配置模板配置进去，在include云WAF的配置模板时，需放到nginx.conf文件最后面。

```
root@5a7b541159f4:/# cat /etc/nginx/nginx.conf
user nginx;
worker_processes auto;

error_log /var/log/nginx/error.log notice;
pid /var/run/nginx.pid;
load_module /etc/nginx/nginx_1.21.6_http_waf_agent_module.so;

events {
    worker_connections 1024;
}

http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    sendfile on;
    #tcp_nopush on;

    keepalive_timeout 65;

    #gzip on;

    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/template.conf;
}
root@5a7b541159f4:/#
```

步骤6. 根据实际云WAF部署情况，修改template.conf引流配置文件。server配置表示把经过此nginx的流量引流到云WAF检测节点进行业务防护，填写的server IP为云WAF检测节点的IP，端口默认从6970开始依次递增，一个检测节点有多少核CPU，就可以配置多少个端口，如下图为2核的检测节点。

```
root@5a7b541159f4:/# cat /etc/nginx/template.conf
upstream waf_server {
    hash $remote_addr$remote_port;
    keepalive 512;

    #custom by cpu nums
    server 10.243.3.88:6970;
    server 10.243.3.88:6971;
}

waf_agent /waf_detect;
waf_agent_request_body_max_size 1m;
waf_filter /waf_detect;
waf_filter_buffer 1m;
waf_filter_reply_body_max_size 1m;

server_include {
    location /waf_detect {
        internal;
        waf_pass waf_server;
        waf_pass_connect_timeout 1s;
        waf_pass_read_timeout 1s;
        waf_pass_send_timeout 1s;
    }
}
root@5a7b541159f4:/#
```

⚠ 注意:

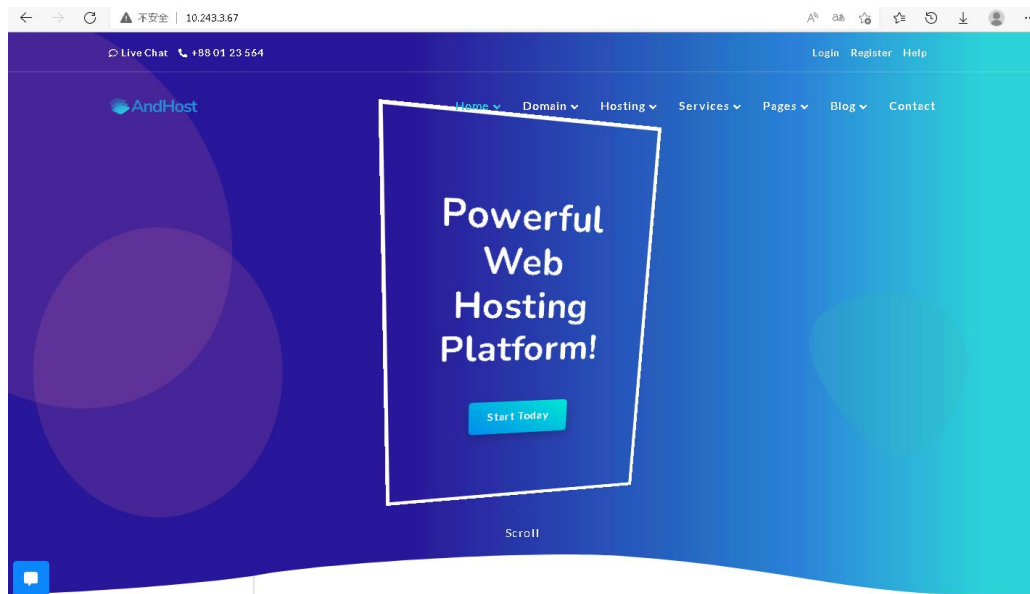
一个 nginx 可以配置多个检测节点的 IP。例如部署了 2 个 WAF 检测节点，一台检测节点有 2 核 CPU，一台检测节点有 4 核 CPU，则配置如下：

```
#custom by cpu nums
server 10.246.84.125:6970;
server 10.246.84.125:6971;
server 10.246.84.126:6970;
server 10.246.84.126:6971;
server 10.246.84.126:6972;
server 10.246.84.126:6973;
```

步骤7. 配置完插件后，重新启动nginx服务，让引流插件才能生效。

4.2.1.4. 效果预览

使用浏览器访问Web站点可以正常访问。



模拟进行攻击，成功拦截，并可以查询到安全日志。



安全日志

时间范围: 2022-04-20 17:00-2022-04-20 23:59

日志类型: http, https

序号	时间	日志类型	威胁类型	源IP
1	2022-04-20 17:28:31	Web应用防护	SQL注入	10.243.3.56
2	2022-04-20 17:28:31	Web应用防护	SQL注入	10.243.3.56

详情

基础信息

时间: 2022-04-20 17:28:31 | 协议: HTTP | 类型: SQL注入

方法: GET | 拦截状态码: - | 严重等级: 中危

动作: 拒绝 | 匹配签名: 漏洞防护

URL: 10.243.3.67/?id=1;select username from userinfo where userid=1

描述: 攻击语句: ;select username from u

危害说明: 攻击者利用此漏洞盗取数据库中的数据，导致WEB业务信息泄露，危及数据库账户信息安全。

规则ID: 16020047

规则名称: select语句SQL注入攻击

检测节点: waf-127.0.0.1

源IP: 10.243.3.56 | 源端口: 60640

源IP归属地: - | XFF IP: -

数据包

INCLUDE ENCODING TYPE: URL

REQUEST:

```
GET /?id=1;select username from userinfo where userid=1 HTTP/1.1
Host: 10.243.3.67
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36 Edg/100.0.1185.44
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
```

5. 常见问题

5.1. 云 WAF 依赖包安装常见问题解决办法

1. 存在低版本docker-ce，导致安装失败。

解决办法：卸载低版本docker-ce再进行安装。

```
yum remove -y docker-ce
```

2. 存在低版本docker-compose，导致安装失败。

解决办法：删除docker-compose二进制文件，再次安装依赖包。

```
sudo rm /usr/local/bin/docker-compose
```

5.2. 云 WAF 安装常见问题解决办法

1. 安装云WAF失败报错如下。

```
[root@localhost tmp]# chmod +x WAF8.0.60_20220415.pkg
[root@localhost tmp]# ./WAF8.0.60_20220415.pkg
Please enter the mount path: /data
Unable to install WAF, reason: Firewalld is not stop, Please stop and disable firewalld
Unable to install WAF, reason: Selinux is not disabled, Please close and disable Selinux
```

解决办法：关闭防火墙和SELinux。

- 关闭防火墙：systemctl stop firewalld.service
- 永久关闭防火墙：systemctl disable firewalld.service
- 关闭 SELinux：setenforce 0
- 永久关闭 SELinux：vi /etc/selinux/config，将 SELINUX=enforcing 改为 SELINUX=disabled，并重启设备。

2. 当管理节点的IP、端口、证书或者Token有变化时，需要同步修改检测节点的配置才能正常接入管理节点。

解决办法：在检测节点宿主机后台输入monitor config，选择需要修改的参数，所有参数修改好后，选择Confirm确认提交，等待后台修改完成重新连接管理节点。

3. 插件部署模式下，如果升级了nginx服务，却没有重新适配so插件库，则引流将不生效。

解决办法：需要重新选择对应版本的so插件库进行安装适配，请参考[2.3章节](#)和[3.3章节](#)。

4. 正常安装了WAF，但是控制台无法登陆，业务不通。

解决办法：有可能是因为WAF的容器网络与平台网络或者客户业务网络有冲突，WAF容器网络默认IP网段为：10.249.249.240/28，请联系400-630-6430处理。

5. 如何卸载云WAF。

解决办法：

在云WAF的宿主机执行monitor uninstall，选择需要卸载的角色，如果当前主机上安装部署了管理节点和检测节点，则需要选择卸载哪种角色。

```
[root@waf-fefcfe0dd06a home]# monitor uninstall
Deployment Role: Management Platform + WAF Agent

Use the arrow keys to navigate: ↑ ↓ → ← and / toggles search
Select Module to be Uninstalled
  * Uninstall All
    Uninstall WAF Agent

----- Selected Module -----
Uninstall All
```

根据提示输入密码（与安装密码一致）。

```
[root@waf-fefcfe0dd06a home]# monitor uninstall
Deployment Role: Management Platform + WAF Agent

Selected Module: Uninstall All
Password to Uninstall: *****
[+] Running 4/4
# Container waf_redis    Stopped
# Container waf_detect   Stopped
# Container waf_mgt      Stopped
# Container waf_nginx    Stopped
Going to remove waf_nginx, waf_detect, waf_redis, waf_mgt
[+] Running 4/4
# Container waf_mgt      Removed
# Container waf_nginx    Removed
# Container waf_detect   Removed
# Container waf_redis    Removed
Untagged: waf_nginx:8.0.60.308B
Deleted: sha256:b6b1014134acd121d736a6ad7b2bc358140dfdaa3fd5210827690275fdb70f97
Deleted: sha256:c5b6fdaf7792f066efaa72f3c5d46cb31d76cde1580d9b5f42f9e1d39c50b451
Deleted: sha256:181a37e0176d63762df9f4ba52bc003a258c996d12ee36d545b2525e6086ac1e
Deleted: sha256:cb9826d912cc07dc6b870001d6fb84ca9adcb7007af94269f9e6e3206f146fe5
Deleted: sha256:89ffc978fa6f33a518fec15dcb9282689b75804d0761a48cb957362e901db4f2
Deleted: sha256:6882c6a9dad9ab09b1e5d5e058324a471e437a00a2c07dd6bc67981221fb571b
Untagged: waf_detect:8.0.60.308B
Deleted: sha256:cd256ae825617841d41d10bf19ab6139746bb83ac13809229933679a43130b63
Deleted: sha256:151f372b96e628afeb2fe9f252b799c6f43719d6b8d97242df457b87500fb556
Deleted: sha256:34c3216c4048cc8684d2fa2595ab41711d0dd102c2b52c56c903ea21a2d5bcf
Deleted: sha256:647e93dd000755c2d1c2dd97e12fbd2363d3146af23dd5da92c59da47e0279e4
Deleted: sha256:d09592b3ba6c6ea467a1599e54acfee8da35815c17fc8340a43795fd5064912c
```

6. 注意事项

1. 宿主机上仅支持单独部署WAF服务，不支持存在用户其他任何业务。
2. 插件模式下，反向代理的相关功能（如SSL卸载等）均由Nginx/tengine服务器完成，云WAF仅对业务流量进行安全检测。
3. 安装云WAF前需要关闭firewalld和SELinux，否则无法安装云WAF。
4. 用户日志数据挂载盘最小要求64G，且不能挂载在根路径下。
5. WAF依赖包安装时，会列表展示出要**卸载**和安装的宿主机程序，请确认后再进行下一步。
6. 云WAF部署完毕后，不要对firewalld 和iptables进行更改，否则可能影响云WAF正常运行。