

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

由于产品版本升级或其他原因,本文档内容会不定期进行更新,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	<u> </u>	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
窗口夕 苦畄夕竿	方括号"[]"	弹出[新建用户]窗口。
図 口 名 、 米 早 名 寺		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	
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	
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	
2.3. 插件环境要求	
3. 设备部署	
3.1. 创建虚拟机	
3.1.1. 私有云环境	
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	
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	
3.7. 集群部署	
3.7.1. 分离式设备反向代理模式集群	
3.7.2. 分离式设备插件模式集群	
4. 基本功能配置	84
4.1. 反向代理模式	
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	
4.1.4. 一个 HTTP 端口负载多个 HTTP 站点防护配置案例	110

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

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, 目 下; Cent OS 系统/var 目录推荐 15G 目 以上。		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。

如下是云WAF提供的so插件库列表:

序号	类型	版本	插件名称
01		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	Nginx	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。

深信服企业级云 SANGFOR a Cloud 6.3	首页	止的机	1网络与安	全存储	实体机	可靠服务	系统管理		
HCI虚拟机 VMware虚拟机									
		O 81 #	⊕新増	2 新增分组		1三排序 ~	•••更多操作	 	
 Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ □ □<td>安WAF8.0 CPU 内存 連急使用家</td><td>50 10% 96% 12%</td><td>新 云(<u>CPU</u> <u>四</u>彦 聖曲使用] 王</td><td>増速拟机 普通度初初</td><td>新虚拟机 racle单机 AP HANA 行业应用 ></td><td>3</td><td> ① 素粉末存在 23 g 克隆虚拟机 Oracle RAC </td><td>导入虚拟机 SQL Server</td><td></td>	安WAF8.0 CPU 内存 連急使用家	50 10% 96% 12%	新 云(<u>CPU</u> <u>四</u> 彦 聖曲使用] 王	増速拟机 普通度初初	新虚拟机 racle单机 AP HANA 行业应用 >	3	 ① 素粉末存在 23 g 克隆虚拟机 Oracle RAC 	导入虚拟机 SQL Server	

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。

	存储位置:	虚拟存储卷1			~	
	存储策略:	2副本默认策略	ł		~ (
	运行位置:	<自动选择>			~	
	操作系统:	CentOS			~	
	重要虚拟机:	🗌 优先保障该虚	拟机的资源使用和故障	恢复 🕕		
硬件	高	级				
快速昏暗: 個酒	7 标配	高配	☑ 启用			Â
📃 处理器	2核		连接到:	默认物理出口 …	A.	
••• 内存	4 GB		高级选项			
━ 磁盘1	120 GB		网卡型号:	Intel E1000	~	
○ 光枢1	无光盘镜像		MAC地址:	FE:FC:FE:30:3D:EB	0	
🕶 eth0	连接到: 默认物理出		IPv4设置:	安装虚拟机性能优化工具后	i, 设置才会生效 查看支持	的系统
				□ 使用以下IP地址 ①		
端 其他硬件				7网*******		
				于网理归:		-

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。

深信服企业级云 SANGFOR aCloud 6.3	首页	虚拟机	网络与	安全存储	实体机	可靠服务	系统管理
HCI虚拟机 VMware虚拟机			(t)- 				
■ 按分组显示 >		€₩	↔新増	+ 新增分组	📑 批星管理	ا⊒ ≢∉ ∨	•••更多操作
と 目 捜索分組 Q						Œ)集群共存在23台部
□ 唐秋桃 (57) CX (19) □ QJJ (15) 设备 (8)	新运维虚拟机-10.24	13.3.56	centos	则试	deepin	XHACK_¥	奶~-10.243.3.62
zHJ (10) zHJ (10) atrust_image (1) wym (5)	CPU 内存 磁盘使用率	0% 25% 24%	▶ 开机 安装系统	□ 关机 ・・・ 更多	已关机	Ē	民关机

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<u>3.2章节</u>。

\$	安装操作系统
人ISO镜像文件安装	人USB设备安装
り 重新加载ISO よ 本地上传	→ 从共享路径获取 搜索ISO
OcentOS-7.9-x86_64-Everyt	hing-2009.iso(虚拟存 立即安装

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]。

vmware' ES	Xi [~]	
"曾 导航器	🗆 📋 localhost.localdo	main
 ■ 主机 管理 监控 ● ごを採机 ● 日存储 ● Q 网络 	 □ 主机 ③ 主机 ④ 创建注册虚拟机 在此主机上创建或注 ◎ 关机 ○ 美机 ○ 新引导 ○ 振务 ○ 振务 ○ 近入维护模式 ○ 锁定模式 	nver 1 创建注册虚拟机 1 关机 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	🔒 权限	SANGFOR
	••• 牛成支持句	BM6000D
		12 CPUs x Intel(R) Xeon(R)
	画 内存	23.97 GB
	▶ 🔓 虚拟闪存	0 B 已用, 0 B 容量
	▼ 🧕 网络	
	主机名	localhost.localdomain

步骤2. 选择创建类型为"创建新虚拟机"。

🔁 新建虚拟机 - wafcentso7.9 (ESXi	6.5 虚拟机)	
 ✓ 1 选择创建类型 2 选择名称和客户机操作系统 3 选择存储 	选择创建类型 您要如何创建虚似机?	
4 目定义设置 5 即将完成	创建新虚拟机 从 OVF 或 OVA文件都图虚拟机 注册现有虚拟机	此运项将指导您完成创建新居识机的过程。您可以自定义处理器、内存、网络连接和存储。创建之后您需要安装客户机量作系统。
vm ware [®]		
		上一页下一页完成取消

步骤3. 配置虚拟机的名称与操作系统为Linux、Cent OS 7。

 ✓ 1 选择创建类型 2 选择名称和客户机操作系统 3 选择左键 	选择名称和客户机, 指定唯一名称和操作系统	操作系统	
3 西非存储 4 自定义设置 5 即将完成	名称 wafcentso7.9		
	虚拟机名称最多可包含 80 个在此处标识客户机操作系统	Y字符,且名称在每个 ESXI 实例中必须是唯一的 可让向导为操作系统的安装是供适当的默认值。	•
	兼容性 客户机操作系统系列	ESXi 6.5 虚拟机 Linux	• •
	客户机操作系统版本	CentOS 7 (64 位)	•

步骤4. 选择虚拟机的存储位置。

□ 新建医外机 - warcentso7.9 (ESAT 1 选择创建类型 2 选择名称和客户机操作系统 3 选择方体	选择要存储 选择要存储 通道和磁盘文件的数据存储。										
4 自定义设置	可从您选择的目标资源中访问以下数据存	储。为虚拟机配	置文件	和所有處	以磁力	助选择目标	数据	字储。			
5 即将完成	名称	~ 容量	~	可用	~	类型	~	精简置备	\sim	访问	~
	datastore1	924 GB		158.87 G	8	VMFS5		受支持		单个	
											1项
vmware [*]											

步骤5. 配置虚拟机的CPU、内存、磁盘空间,参考<u>2.2章节</u>,最低2C4G,并配置网 卡连接到相应的位置。

选择创建类型 选择名称和客户机操作系统 选择存储	自定义设置 配置虚拟机硬件和虚拟机附加选项			
自定义设置	虚拟硬件 虚拟机选项			
	📃 添加硬盘 📷 添加网络适配	器 📄 添加其他设备		
	► 🔲 CPU	2 🔻 🚺		
	▶ 🎫 内存	4 GB 🔻		
	▶ 🚍 碩盘 1	140 GB 🔻		0
	▶ 💽 SCSI 控制器 0	VMware Paravirtual	•	0
	Marca SATA 控制器 0			0
	🚭 USB 控制器 1	USB 2.0	•	
	▶ ■■ 网络适酉器 1	VM Network	▼ <mark></mark> ☑ 道	接
	▼ 🗐 CD/DVD 驱动器 1	主机设备	×	0
vm ware [®]	状态	☑ 打开电源时连接		

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

选择创建类型 选择名称和客户机操作系统 选择存储	自定义设置 翻畫感知頓件和感知和地运项			
自定义设置 即将完成	虚拟硬件 虚拟机选项			
	🔜 添加硬盘 📷 添加网络适西器	🔤 添加其他设备		
	🕨 🖬 CPU	🔜 新硬盘		
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	🔜 现有硬盘	-	
		■■ 网络适香器		
	▶ 🛄 碩盘 1	CD/DVD 驱动器		0
	▶ 🐼 SCSI 控制器 0	📄 软盘驱动器		0
	ama SATA 控制器 0	回回 串行端口		0
	➡ USB 控制器 1	 ・ ・	•	
	▶ ■■ 网络适酉器 1	Bas USB 设备		☑ 连接 🛛 🛞
	▼ 🞯 CD/DVD 驱动器 1	声音控制器	•	0
vm ware [®]	状态	Mail PCI 设备		
		🐼 SCSI 控制器		
		SATA 控制器		Signation of the second

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。

虚拟硬件 虚拟机选项				
📃 添加硬盘 💼 添加网络适配器	📑 添加其他设备			
F 🔲 CPU	2 🔻 🚺			
▶ ़ 内存	4 GB •			
▶ 🛄 碩盘 1	[140] GB ▼			0
▶ 🛃 SCSI 控制器 0	VMware Paravirtual	٠		0
sama SATA 控制器 0				0
♥ USB 控制器 1	USB 2.0	•		
▶ ■■ 网络适置器 1	VM Network	•	🗹 连接	0
▼ 🗐 CD/DVD 驱动器 1	主机设备	*		0
状态	主机设备 数据存除180 文件			
	kulver Linex	本加減化 ● 添加減化設备 添加減金 ● 添加減化設备 ● CPU 2 ● G 0 ● 硬盘1 140 ● G ● ● 磁盘1 140 ● G ● ● G ● ● G ● ● G ● ● G ● ● G ● ● G ● ● G ● ● G ● ● G ● ● G ● ● USB 控制器 1 USB 2.0 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	□ 添加現金 添加現金通路 □ 添加現金設备 □ CPU 2 • ■ GPF 4 0B • • ■ 硬盘 1 140 GB • • ■ ● SCIP 2 • • • • ■ ● ○ CD/DVD 驱动器 1 ±/USB • • • ★ ★/USA ★/USA ★/USA ★/USA	添加現金 添加現金通路 添加其他设备 添加現金 添加其他设备 Image: CPU 2 Image: CPU Image: CPU

🔂 数据存储浏览器				
	除 🔒 移动 👔 复制 🞦 创建	目录 📔 🤁 刷新		
 datastore1 vrnimages 	Centos7.3_Gnome centos7.3_Minimal centos7.9 centos7.9_1 centos8.5_Gnome cwy ggt sentos8.5. g m	 7.3-CentOS 7.9-CentOS CentOS-8.5 		
	 ⑦ 打开 ← → · ↑ → 比 组织 ▼ 新建文件夹 	ー 电脑 > Desktop > 安装部署需求材料 > w	raf导入镜像	∨ ひ 搜索
[datastore1] cwy/	↓ 快速访问 Desktop 下载 My Docume ★ 同 图片	名称 ◎ 7.9.iso ぽ 機板 pkg-IP-CentOS-8.3.2011.ova	修改日期 2021/11/9 20:18 2021/11/4 17:54	美型 光盘映像文件 开放虚拟化格式分发

步骤8. 文件上传完成后,选择上传的Cent OS7的ISO镜像文件

datastore1 Centr vmimages cento cento cento	tos7.3_Gnome os7.3_Minimal	7.3-CentOS 7.9-CentOS		
CVV Qt Qt SPT VAF VAF VAF VAF VAF VAF	os7.9 os7.9_1 os8.5_Gnome os8.5桌面 _CW _qqt 807.1044 1 3 8.0.28_for_ecl III	j CentOS-8.5	7.9-CentOS-7-x86_64 4.39 GB 2021 年 12 月 21 日 星	

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<u>3.2章节</u>。

 1 选择创建类型 2 选择名称和客户机操作系统 3 选择存储 	即将完成 在完成向导之前查看您的设置选择	74
4 自定义设置 5 即将完成	置备类型	new
	名称	wafcentos7.9
	数据存储	datastore1
	客户机操作系统名称	CentOS 7 (64 位)
	兼容性	ESXi 6.5 虚拟机
	VCPU	2
	内存	4 GB
	网络适西器	đ
	网络适西器 1 网络	VM Network
	网络适西器 1 类型	VMXNET 3
	IDE 控制器 0	IDE 0
	IDE 控制器 1	IDE 1
	SCSI 控制器 0	VMware Paravirtual
	SATA 控制器 0	新的 SATA 控制器
Man	碩盘1	
VIIIWare	容量	120GB

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。

www.uxwei 华为云	最新活动	产品 解决方案	EI企业智能 定价 云市场 合作伙伴	开发者 支持与服务 了解华为云	提案 Q :
	搜索产品	Q	计算		
	精选推荐	应用中间件	弹性云服务器 ECS HOT 可随时自动获取。弹性伸缩的云服务器	GPU加速云服务器 GACS 提供GPU计算资源的弹性云服务器	FPGA加速云服务器 FACS 提供FPGA计算资源的弹性云服务器
	计算	开发与运维	裡全庫服冬哭 RMS	云毛机 CPH	专屋主机 DeH
	容器	企业应用	高性能、高安全的云上物理服务器	具有虚拟手机功能的云服务器	专属物理主机创建的云服务器
	存储	视频	弹性伸缩 AS	镜像服务 IMS	函数工作流 FunctionGraph
	网络	安全与合规	根据预设策略自动调整计算资源的服务	提供完善的镜像管理能力	自动运行代码,无需配置或管理服务器
	CDN与智能边缘	管理与监管			
	数据库	迁移			
	人工智能	区块链			
	大数据	华为云Stack			
	IoT物联网	移动应用服务			

步骤2. 点击<立即购买>, 跳转购买页面。

www. 华为云	● 最新活动 产品 解决方案 印企业管税 定价 云市场 合作伙伴 开发者 支持与服务 了解华协云	搜索 Q 文档 葡萄
	弹性云服务器 ECS 概成 产品功能 走价 实例类型 杨果与实践 入门 资源 ~	性的专业研究
	弾性云服务器 ECS ④ 独主最終題(Llauk Cloud Server, ICS)是一や五上可循时自動形成、可強性伸進的计算服务,可解如何打造会会、 可象、反系、高级的应用形成。 型理物合 解和文档 解和文档	
	了解弹性云服务器ECS	
	30+年 多样性算力 200+ 80+ 华为湾县身石(T董磁和设施原端 支球X86、整篇、算篇、异构 支持X06小企业应用场景、属坦 80+ 30多年的技术、能力、经验用 园大类型算力,提供更优属力 各类业务的上云需求 中立、安全、可信的云振务 繁全入中均云 造彩 84%	1110日エルネルロイエンムのご用。和JJJビンビルは、現ケイ 天主机限时化派、現天不到0.73元 工即枪動

步骤3. 购买ECS服务器, 配置购买服务器参数

序号	参数	说明
		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。 ● 句年/句月
01	计费模式	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。
		 竞价计费 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。
02	区域	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。
03	可用区域	可用区是在同一区域下,电力、网络隔离的物理区域,可 用区之间内网互通,不同可用区之间物理隔离。 一个区域内有多个可用区,一个可用区发生故障后不会影 响同一区域内下的其它可用区。
		部署云 WAF 选择 x86 计算架构。
04	计算架构	 x86 计算 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。 鲲鹏计算
		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

		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
		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。
07	主机安全	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。
		个问虚拟私有云里面的弹性云版务畚网络為认个迪。
		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。
10	网卡	 主网下 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。
		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。
11	安全组	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。
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相通信。 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,若部署环境中有 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。

J+LI 4N38050 hr	目定义购头	weav.														
O HEART	2) RIBE	n (3 aw	em — (4) and dette												
计器模式	638	E/BLA BOOK	it#	寬約計畫	0											
医端	♥ \$\$限-	广州 •	◎ 推荐区域 🗯	\$ 华北-马兰殿布-	- (0) 👘 西	5期-費阳— (0)	\$4北-北東四	(0) 绿阑-广	∽州 (0) 绿东	上海						
	不同区域的	云服务产品之间内同互不相	B通:请就近选择数	近您业务的区域。	可减少网络约瑟	疑、提高访问速度	, 如何透频区划	1								
可用区	161 E	1.9f2 可用	126	可用区3	可用回	2 5	可用区2	0								
CPU%转载	x86113	1 KBH1 ()				m#			-014-01-01		0					
CPU補助 规格	x86117 最終成初 週用计1		vCPUs 全部 1 内存优化型	超大內存	▼ 型 液性純	内存 全部 約十算型 初	电带强型	▼ 超商1/0型	現格名称 GPU加速型	FPGA201822	Q	通用入门型	0			
CPUMER; 规M	x86110 Ref. 671	(4)時日期 ③ (4)時日期 ③ (1)時代(1) (2)時代(2) (3)時代(2) (3)時代(3)	vCPUs 全部 1 内存优化型	L 超大内存的	▼ 型 商性創 s 内存(GiB) 」	内存 全部 約1算型 初 JE	CPU (E	▼ 超商1/0型	現格名称 GPU加速型	FPGA201度型 基准 / 最大带成	D Esoura EL ©	通用入门型	0	内间收发泡 ① JE	网络香蕉松 ③ 1日	
CPUMRES	x8611月 最新乐行 通用计1		vCPUs 全部 2 内存优化型	U 超大内存的 VCPU: 2VCPI	▼ 型 飛性線 > 内存(GiB) ↓ US 4 GiB	内存 全部 16计算型 超 18	色潮浸型 CPU 1日 Intel Ice	マ 超庵I/O型 E Lake 3.0GHz	現後名称 GPU加速型	FPGA加速型 基础 / 最大带成 最大 4 Gbit/s	D Estatia EL ©	通用入门型	0	内网络发行图 ⑦ J王 400,000	援防奈考約 ③ JE 20.50/Jet	
CPU移动 规图	x86117		vCRUs 全部 1 内存优化型	i 超大的种 vCPU: 2vCPI 2vCPI	▼ 型 飛性網 ≤ 内存(GiB) J US 4 GIB US 8 GIB	内存 全郎 6计算型 初 JE	史憲領型 CPU 1日 Intel Ice	・ 超潮()の型 E Lake 3.0GHz Lake 3.0GHz	规格名称 GPU加速型	FPGA加速型 基准/最大带版 最大 4 Gbit/s 最大 4 Gbit/s	Q Estata E	通用入门型	0	内网络发短 ② J王 400,000 400,000	線路巻考約 ③ J亜 100.50(小計 100.708/小計	
CPUMRIG	x001111 最新系列 通用111		vCPUs 全部 1 内存优化型	2	▼ 型 務性部 US 4GB US 4GB US 8GB US 8GB	内存 全郎 約十算型 码 JE	色潮通型 CPU JE Intel Ice Intel Ice	マ 超売いの型 Lake 3.0GHz Lake 3.0GHz Lake 3.0GHz	現後起称 GPU加速型	FPGA加速型 基准 / 最大带端 最大 4 Gbit/s 最大 4 Gbit/s 最大 8 Gbit/s	D Esaita EL ③	通用入门型	٥	AMMAX281 ③ JΞ 400,000 400,000 800,000	和10.999/小41 20.59/小41 20.59/小41	
彩版 PDM	xx001171 最新系列 2月日日 () () ()		vCPUs 全部 内容优化型	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	東世朝 素 内存(GIB) J US 4 GIB US 8 GIB US 8 GIB US 8 GIB US 16 GIB	内存 全郎 6计算型 砲 JE	会潮過型 CPU 1日 Intel Ice Intel Ice Intel Ice	マ 記載でいつ型 にはな 3.0GHz にはな 3.0GHz にはな 3.0GHz にはな 3.0GHz	現後名称 GPU加速型	FPGA加速型 基准 / 最大帶廠 最大 4 Gbit/s 最大 8 Gbit/s 最大 8 Gbit/s	Q AUDEE BL ③	通用入门型	٥	ASSR40202151 ③ 1日 400,000 400,000 800,000 800,000	線路参考後 ② J王 100.50(사람 100.758(사람 100.758(사람 100.758(사람 100.758(사람 100.758(사람 100.758(사람 100.758(사람 100.758(
591 1938	xxxxi x x x x x x x x x x x x x x x x x		vCPUs 全部 内存优化型	i 超大内研 vCPU 2vCPI 2vCPI 2vCPI 4vCPI 4vCPI 4vCPI 8vCPI	▼ 型 所住線 は 内存(G(B) 」 US 4 G(B US 4 G(B US 8 G(B US 8 G(B US 16 G(B US 16 G(B	内存 <u>全部</u> 8计算型 初 JE	etatistatistatistatistatistatistatistati	・ 記載いの型 E Lake 3.0GHz Lake 3.0GHz Lake 3.0GHz Lake 3.0GHz Lake 3.0GHz	現他名称 GPU加速型	FPGA30/感型 基础 / 最大帶廠 最大 4 Gbit/s 最大 8 Gbit/s 最大 8 Gbit/s 最大 15 Gbit/s	D AIDEE	通用入门型	0	рыянсаете () да 400,000 800,000 800,000 1,500,000	第10550/041 第0550/041 第0550/041 第0550/041 第1550/041 第1550/041	
69UMR	xx011行 最新度列 2月用计 0 0 0		vCPUs 全部 1 内存付代型	 超大の将辺 VCPU 2xCPI 2xCPI 2xCPI 4xCPI 4xCPI 4xCPI 8xCPI 8xCPI 	▼ 型 酸性線 は 内存(GB) J US 4 GB US 8 GB US 8 GB US 16 GB US 16 GB US 16 GB US 16 GB	内存 全部 約4頁型 砲 1日	空部浸出 CPU J目 Intel Ice Intel Ice Intel Ice Intel Ice Intel Ice Intel Ice	* &SREVOTA E Lake 30GHz Lake 30GHz Lake 30GHz Lake 30GHz Lake 30GHz	現務名称 GPUIDIE型	FPGA100回型 基础 / 最大带窗 最大 4 Gbit/s 最大 8 Gbit/s 最大 8 Gbit/s 最大 15 Gbit/s 最大 15 Gbit/s	D Beans EL ()	通用入门型	0	яряесяте () де 400,000 800,000 800,000 1,500,000 1,500,000	제46년 1940 ① JE 10050/041 10050/041 10050/041 10050/041 10050/041 1006/041 10150/041 1006/041	
67U3860	x0011初 風射系列 (回日) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	KBBH#R O Image: State Stat	vCRU3 金藤 21 内容依依置	 超大内容が くCPUB 2xCPI 4xCPI 4xCPI 8xCPI 8xCPI 12xCl 	T Television T Television J S PSPF(Gib) J US 4 GiB J US 4 GiB US 8 GiB US 16 GiB US 16 GiB US 16 GiB US 16 GiB US 12 GiB PUS 22 GiB PUS 24 GiB PUS 24 GiB PUS 24 GiB PUS 24 GiB	内存 全部 約4算型 初 1日	史神過型 CPU J를 Intel Ice Intel Ice Intel Ice Intel Ice Intel Ice Intel Ice	・ ・ ・ ・ ・ ・	現格名称 GPU加速型	FPGA32进型 基度/最大带函 最大 4 Gbits 最大 8 Gbits 最大 8 Gbits 最大 15 Gbits 最大 15 Gbits 最大 15 Gbits	D EL ③	通用入门型	0	ранкоже © 42 400,000 800,000 1,500,000 1,500,000 1,500,000 2,000,000	総合参考会 ② JE 1 20550(少年) 1 20578(小年) 2 20599(小年) 2 1597(小年) 1 1598(小年) 2 1597(小年) 4 25997(小年)	



深信服云 WEB 应用防火墙快速安装手册

网络	vpc-10.0.1.0网经 (10.0.1.0/2	(4) * C subnet-	88e3 (10.0.1.0/25)	 C BADMEPREZE 	• • • • • • • • • • • • • • • • • • • •		
	如谐创建新的唐拟私有云,却可	可前往控制台创建。					
广展 用卡	 第四一共同本 想还可以消 	翻1 块网中					
2全组	군WAF (b4cc91c4-03e2-4d	4a-b383-f483bca6dde7) 🔘	• C 新建安全组 C	D			
	安全組美級防火績功能。是一 清濃保新防安全線已於溝22線。	○運輸上的分組、用于设置网络访问 ○ (Linux SSH巻巻)、3389時〇 (控制。 Windows洗焊巻巻)和 ICMP:	物设(Ping)。 配器安全研想到			
	障礙安全追切別へ						
	降職安全追規则 へ 入方向規則 出方II	向规则					
	降康安全组织则 へ 入方向规则 出方I	向规则					
	P#康安全组织则 ^ 人方向规则 出方 1 安全组织称	向规则 优先级	旅展	物设施口	英型	源地址	職送
	降康安全追视则 へ 入方向规则 出方(安全相称称	向规则 优先级 1	錠路 元に	物役論日 TCP: 80	美型 IPv4	源地址 0.0.0.00	180.5
	降嚴安全追羽則 ∧ 入方向規則 出方1 安全相称称	向规则 代先级 1 1	第 第 第 第 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	10/03/8/21 TCP: 80 TCP: 443	英型 IPv4 IPv4	湖市地址 0.00.00/0 0.00.00/0	滅 ぎ
	操業全部規則 入方向規則 安全規株件	向规则 优先级 1 1 1	施服 九年 九年 九年	16003862 TCP: 80 TCP: 443 TCP: 22	英型 IPv4 IPv4 IPv4	2015年 2000月	188 - - -
	降都会自然的 入方向規則 学会相称中 EWAF	的规则 依先级 1 1 1 1 1 1 1 1	加朗 た計 た計 た計 た計 た計 た計 た計	160000000 TCP: 400 TCP: 443 TCP: 22 TCP: 4431	交型 IPv4 IPv4 IPv4 IPv4	2000/0 0.0.0.0/0 0.0.0.0/0 0.0.0.0/0	905

线路	全动态BG	P	静态BGP	(0					
	⊘ 不低于99.95%	6可用性保障	₿.							
公网带宽	按带] 流量软	きけ 妻 🖒 大 或 较 絶 が	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 务流量错峰分布场景	0
	指定带宽上限,拍	安际使用的	的出公网流量计	+费,与使用	目时间无关。					
带宽大小	5	10	20	50	100	自定义	- 1	+	带宽范围: 1-300 M	bit/s
	⊘ 免费开启DDo	S基础防护								

云服务器名称	ecs-10fd 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	密码 密钥对 创建后设置
用户名	root
密码	请牢记密码,如忘记密码可登录ECS控制台重置密码。
	请输入密码
确认密码	请再次编入密码
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。
	现在购买 使用已有 暂不购买 ⑦
天吃捡	
Amir	
	Example (
云服劳酷组 (ባ远)	

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<u>3.3章节</u>。

								O'HO O'KA U	desiration () in the	
335			建议是约门持续	進升产局体验的展动力,感谢到	的参与1					
		746, X46, MHX66, F4 *								cler
·服主机		教以接觸名和教堂								
全國服务器		8務/ID	210	可用区 🏹	865 V	规位/用限	19181E	计变模式 🎖	标签	操作
·谜面		RCS-6074	8	可用区3	0 (\$ff=	123.60 (SPIE(SR) 100	0 Mbit/s 123.60mls 🚽 (39125)	8. () 終発計算		6899
9篇分布式存储		130089C-1030-4110-9083-8/12				194. TOKINE BE (BARRE)	192.1035(nim((c;s))	2022	22/43 BL	
18日5										
时生冲探										
1001	1									
服务器组										
E助模板 NEW	1									
.能购买组 NEW										
19816	1									
20.94920 H10204	<u>,</u>									
性公用 (P	-									

3.1.2.2. 腾讯云

🔗 腾讯云	田町 最新活动 产品 解决方案	定价 企业中心	云市场	开发者	客户支持	合作与生态	了解腾讯云		
	品 查看全部产品	(搜	索产品名称	τ		٩	云服务器	云原生数据库 TDS
	推荐(HOT)		计算	I		量子技术		边缘计	算
	计算		云服	务器		抗量子签名	服务	边缘计	算机器
	容器与中间件		轻量	应用服务器				物联网	边缘计算平台
	存储		黑石	物理服务器2	0				
	数据库		GPU FPG	I 云服务器 A 云服务器					
	网络与CDN		专用	宿主机					
	视频服务		云托	付物理服务器	I				
	安全		弹性	伸缩					
	大数据		批量	计算					
	人工智能		高性	能计算平台	NEW				
	物联网		本地	专用集群					
			边缘	可用区					
	1211121月与云通信		自动	化助手					
	行业应用								
	开发者服务								

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。

(1907) (1	窦 定价 企业中心 云市场 开发者 畜户支持 合	作与生态 了解腾讯云		新春采购 Q
	▲ 体熱型! 轻型の用肥料器な体なの高す 400m 2019年 つて肥子器 CVM 気酸多番 (Cloud Virtual Machine, CVM) 提供 比容器、适应率体的业务需求、并只需按实际 硬件采购成本、商化 IT 运维工作。	天) 安全可靠的弹性计算服务。您可以实现 使用的资源计费。使用 CVM 可以极大 回价格计算器		
		新春大促 新春特惠、國際聖得國際的6美 轻量加用服务器4核8G首件211元	新企业用户福利专场 销能性现象全化区、元都等需要可 以行音75%的成本	第六代云服务器上线 算力局面进升流,网络性器局面进升3 倍,性价比局面提升3倍目前往购买
		产品推	王存	

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	 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。 包年/包月 包年/包月 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

网站电商小程序 手游/端游 数据库 大数据 机器学习 图形渲染

		估设备需求量的场景,价格相较于按量计费模式更低廉。
		● 按量计费
		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。
		● 竞价实例
		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%。
02	区域	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。 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。
03	可用区域	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。
04	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。
05	实例	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。 云 WAF 的 CPU 内存选型可参考 <u>2.2 章节</u> ,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	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。
08	定期快照	快照可恢复由用户误删,病毒感染等情况导致的数据异常。 部署云 WAF 可以根据实际情况购买或不购买快照功能。
09	公网带宽	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。 部署云 WAF 建议给云 WAF 的 ECS 单独绑定一个弹性 IP,若部署环境中有 NAT 网关等,根据实际环境进行调整。

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。
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。
		免费开通 DDoS 防护和主机安全基础版
16	安全加固	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。
		田石石 WW うちに広方が旧元うたみ小うた日の化功子功 化 化。
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	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 竟价实例 ⑦ 详细对比口
	—— 华南地区 —— —— 华纪地区 —— —— 西南地区 —— —— 港渡台地区 —
地域	广州 上海 南京 <mark>國</mark> 北京 成都 重庆 中国香港
	新加坡 曼谷 雅加达 孟买 首尔 东京 硅谷 弗吉尼亚
可用区	随机可用区 南东一区 22 南东三区 22 ⑦
网络	Default-VPC (読込) v の C 子短期(会百田) 4093へ
rand	当前列络力数以私有网络「子列、建议想得全业名誉要进行调整
	如此有私有网络子网不符合您的要求,可以去控制给 新建私有网络B 或新建子网B。云服务器购买后可以通过控制台切除私有网络完成私有网络子网的切换
实例	2岐 × 4GB ×
	全部加型 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 ⑦
	全部实例类型 标准型S6 标准型SA2 标准型S5 标准存储增强型S5se ^{NEW} 标准型SA3 ^{NEW} 标准型SA1 ^{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 NW 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	公共编集 自定义编集 共享赔偿 镜像市场 ⑦
系统盘	寄性能云硬曲 ∨ - 100 + GB ⑦ 洗励指引 C
	购买成功后,系统血不支持更换介质
数据盘	● 新建云硬盘数据盘 还可增加20块数据量 ⑦
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 C* default-policy/星期四]12:00[保留30天后自动删除 C*
	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 50G8 免费额度,详情可见 快服计费概述 C
公网带宽	✓ 免费分配独立公网IP ⑦
	按带宽计费 按便用流量 ⑦ 详细对比 🗉
	1Mbps 5Mbps 20Mbps 100Mbps 注意:流量素用每小时独算一次,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12

1.选择机型	2.设置主机 3.确认配置信息
安全组	新建安全组 已有安全组 ⑦ 使用描引 2
	请选择安全组 × C
	如您有业务需要的通其他满口,您可以 新建安全组 2
所属项目	默认项目 ~ ⑦
标签 ⑦	标签键 标签值 操作 C
	 可选,请选择一个标签键 可选,请选择标签值 一一、请选择标签值
	添加
	如服有标签标签值不符合物的要求,可以去控制台 新建标签标签值¹²
实例名称	可选,不填默认未命名 支持批量连续命名或指定模式串命名,最多128个字符,你还可以输入128个字符 ⑦
登录方式	设置器码 立即关联器钢 目动生动器码 ⑦ 注: 道中门您所设置的密码、如意点可容要CVM钟制合重要密码、自定义密码的实例不变持保存为启动律板。
田白夕	
用尸石	1001
密码	请输入登录密码 💋
确认密码	请再次输入登录密码 Ø
安全加固	✓ 免费开通 ⑦
	安裝组件免费开通DDoS防护和主机安全基础版 详细介绍也
一些吃	✔ 免费开通 ⑦
ZAMULL	免费开通云产品监控、分析和实施告答,安装组件获取主机监控指标 详细介绍 12
自动化助手	✓ 免费升通 NEW >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
	メネジーンダイルロネルルディングで、スタンロスメディル単単サ大学、アイトドマ、アストレーターとロストメリン第日
定时销毁	一 开启定时销毁 ⑦
	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。

○ 阿里云 最新活动 产品 解决方案 ◇ 云市场 ◇ 台	合作伙伴~ 支持与服务~ 开发者~ 了	解阿里云~	短信	
查看全部产品 >	Q、搜索云产品			
熱门产品 強性计算	云服务器	无影云电脑 >	弹性编排	
存储	云服务器 ECS HOT	无影云桌面	弹性伸缩 HOT	
数据库	弹性裸金属服务器 (神龙)	THE WILL UP .	资源编排	
安全	轻量应用服务器		运维编排 OOS	
大数据	GPU 云服务器	超级计算集群		
人工智能	弹性加速计算实例 EAIS	弹性高性能计算 E-HPC	Serveriess	
网络与CDN	FPGA 云服务器	批量计算	函数计算 FC	
初時音時	专有宿主机	50 BB BD 40	Serverless 应用引擎 SAE	
	阿里云云盒	5000073	Serverless 工作流 NEW	
	弾性云手机 (公测中)	弹性容器实例		
ガスラム地	计算巢服务 (公测中)	容器服务 ACK	上具与服务	
物联网IoT	VMware 服务(公测中)	边缘容器服务	服务器迁移中心 SMC	
混合云		Serverless 容器服务 ASK		
企业服务与云通信	虚拟主机	服务网格 ASM	操作系统	

步骤2. 点击<立即购买>,跳转购买页面。

(一)阿里云 最新活动 产品~	解决方案 ~ 云市场 ~ 合作伙伴 ~ 支持与服	务 ~ 开发者 ~ 了解阿里	∎≂ ~		城名	Q	中国站~ 3	文档 购物车
	山田田田市 学性 仕 算 ・ の で 開 の 、 で の で 、 の の の の 、 の の の の の の の の の	:IT 成本、携升温敏效率 ()線石, 数力子提供永不停打	20世史在14年代	度十一年深草技术和	Č			
	云服务器精选特惠 新用户低至0.52折起,爆款免费试用3个月	ECS 免费试用实(试用中心 月,每人限1次1台	开发表 新用户可事2核2G转	皆成长计划 至星服务器99元/年超低价	云服务器老用 实例升级、续要等	目户礼遇 再任至 6.3折	
	弹性计算 强急、稳定、安全的元计算能力、助力企业上云 云影功器 网络航计算 HPC	容護級务	強性編排	Serverless	操作系统			
	云服务器							

步骤3. 购买ECS服务器, 配置购买服务器参数

序号	参数	说明
		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。
		● 包年包月
01	计费模式	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	 地域 地域指的是 ECS 实例所在的物理位置。 可用区 可用区 可用区-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 <u>硬件资源要求</u> 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	 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 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	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	快照服务	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。 部署云 WAF 可以根据实际情况购买或不购买快照功能。
08	网络	 专有网络 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 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	 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、专有网络类型的和助弹性网卡、NAT 网关和高可用虚拟 IP 上。 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。 按固定带宽 新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。带宽费用合并在 ECS 实例中收取。 按使用流量 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。 部署云 WAF 建议给云 WAF 的 ECS 单独绑定一个弹性 IP,若部署环境中有 NAT 网关等,根据实际环境进行调
		整。 安全组类似防火墙功能,是一个逻辑上的分组,用于设置
10	安全组	安全组类似防火墙切能,是一个逻辑上的分组,用于设直 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。
11	弹性网卡	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。 部署云 WAF 仅需一个主网卡即可,无需额外的辅助网卡。
12	IPv6	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 <u>https://help.aliyun.com/product/85563.html</u> 。 云 WAF 支持 IPv6 的反向代理及防护。
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。

	摄配节省计划,按量	账单最高可	享受 2.4折折扣。	且计划内产品7	不受地域/升降配/颈	(更规格調照#	1),前往介绍了	力了解更多>				
	使用资源保障服务进	行客量預留	, 确保您的应用	拥有扩容所需容。	量、点击了解更多	*						
及可用区	华南1 (深圳)	•	服机分配	可用区 E (1)	可用区 😡	可用区 D	可用区C	可用区 A	可用区 8			
譯地域	不同地域的实例之间	内网互不相	i通: 选择靠近您	套户的地域,可	降低网络时延、福	高忠客户的访	问速度。 🕜					
则格	分类运型 场	展化远型										
格族 審注刑	当前代 所有	任 21	CPU 4 GiB	巴股定例短格								
的地域				Englished and the								
继驾配	雜造 选择 vCPU	• 1	」輝内存 ·	, 搜索规格名	.称,如:ecs.g5.lar	ge Q	1/0 优化实际	例 ⑦ 显示支持	IPvő 🔻			
	规档族⊙	案例规格	VCPU	♦ 内存 ♦	平均基准CPU 计算性朝	处理爵主 须/香烦	内网带宽 💠	内网收发起 ③ 单	存储IOPS 基准/峰值 ①	IPv6	●考价格 ① ◆	处理器型号
	→ 计算型 c7	ecs.c7.la	ge 2 vCPL	J 4 GiB	-	-/3.5 GHz	最高 10 Gbps	90万 PPS	2万/11万	是	¥ 0.448 /Bj	Intel Xeon(Ice Lake) Platinum 83698
	0					2.55	優赛 10					
	O □① AMD 计算 型 c7s	ecs.c7a.li	irge 2.vCPU	J 4 GiB		GHz/3.5 GHz单核	Gbps	90万 PPS	1.25 万/11 万	是	¥ 0.293 /B;	AMD EPYC** Milan 7T83
	AMD 计算 型 c7a 委主频计算 型 H(c7 回	ecs.c7a.k ecs.hfc7.	arge 2 vCPL	U 4 GiB	-	GHz/3.5 GHz単核 3.3 GHz/3.8 GHz	Gbps 最高 10 Gbps	90万 PPS 90万 PPS	1.25 万/11 万 2 万/9 万	12. 12.	¥ 0.293 /85 ¥ 0.471 /85	AMD EPYC** Milan 7783 Intel Xeon Platinum (Cooper Lake) 8369
		ecs.c7a.k ecs.hfc7. ecs.c6e.k	rge 2 vCPI	U 4 GiB J 4 GiB		GHz/3.5 GHz単核 3.3 GHz/3.8 GHz 2.5 GHz/3.2 GHz	Gbps 最高 10 Gbps 最高 10 Gbps	90万PPS 90万PPS 90万PPS	1.25万/11万 2万/9万 2.1万/-	是是	¥ 0.293 /85 ¥ 0.471 /85 ¥ 0.41 /85	AMD EP/C** Milan 7783 Intel Xeon Platinum (Cooper Lake) 8369 Intel Xeon(Cascade Lake) Platinum 8269CY
		ecs.c7a.li ecs.hfc7. ecs.c6a.li	arge 2 vCPI arge 2 vCPL irge 2 vCPL	U 4 GiB J 4 GiB J 4 GiB		GHz/3.5 GHz単核 3.3 GHz/3.8 GHz 2.5 GHz/3.2 GHz 2.5 GHz	最高 10 Gbps 最高 10 Gbps 最高 10 Gbps	90万PPS 90万PPS 90万PPS	1.25万/11万 2万/9万 2.1万/-	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	¥ 0.293 /85 ¥ 0.471 /85 ¥ 0.41 /85	AMD EP/C** Milan 7783 Intel Xeon Pitstinum (Cooper Lake) 8369 Intel Xeon(Cascade Lake) Platinum 8269CY

网络		
公网 IP 公网带恋计器 带宽计数模式 带宽峰值		
安全组 安全組限制 配置安全組	月国王先思議外発電 500x わぎの乳屋交出がみ、 76美 を1歳分が約400 医時を全国 ① 今全国時には久秋石道、月下で国内的に同時利、町名戸Q3時間割分約 新国を全国、全全州Q>	
弹性网卡	主用+ 交通初 (部以)-rev-vc3hc0-bilmyJah2agd/met	
IPv6	您当能无法惊死 Pr-6 (州主查查想原因)	>

登录凭证	密明对 自 定义密码 创建后设置		
登录名	root		
密钥对 ③	· 通過探索領対	○ 金属電磁切り 如何使用密码对	
实例名称	launch-advisor-20220307	如何自己文美并东的东京 ①	
	2~128个字符,以大小写字母或中文开头,可包含数字、点例	F(1)、下划線(2)、半角電号(1)或施字符(-)	
描述	输入描述		
	长度为2~256个字符,不能以http://或https://开头		
主机名 ⑦	操作系统内部的计算机名,远端项	如何自定义有限主机名①	
	Linux 參其他操作系统: 长度为 2~64 个字符,允许使用点号	() 分隔字符或多段,每段允许使用大小写字母、数字或准字符(-) ,但不能追续使用点号() 或准字符(-) ,不能以点号() 或准字符(-) 开头或她尾。	
有序后缀	为 实例名称 和 主机名 添加有序后缀 ⑦		
实例释放保护	前止通过控制台或 API 決制除释故 ⑦		
高级选项(实例 RAM:	角色 & 实例自定义数据 cloud-init) (可点击展开)		

标签	粉蛋曲包分大小與物種微力組成。 認必置始於医供应用在本次含識的全部医例和反晶。 離子粉层也可以是用活动 <mark>管理成本的薄化的</mark> 有分解,设置所压硬 <mark>自动的模定量的位置合组直带分组直控数量,对分组织原进行自动化温速推进。 > 以下为您提供一些不得的她的某用粉层塑像,您可以在由茶塑塑你进图像,并补充适合您的茶屉圈。(何点主算开)</mark>
	他们与卫务 技术与用途 财务分钟
	team company group IRUL 公司 割门 product project app 刻目 並用 user owner role creator 房中 先振人 角色
	- 調節時時間 調節時時間 + 減加時時間
资源组	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
部臀集	約32日本本部 * ○ ②
专有指主机	你可以說出社後他 前 國 专项信 主的 >
私有池容量	10.576.4500 · O

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。
⑦ 天翼云 最新活动 产品 解決方案 云网融合	定价 应用商城 合作伙伴	支持与服务 了解天翼;	Ā	
	搜索产品			
基础云产品	计算	存储	网络	安全
云网融合/网络	弹性云主机 憲 HOT	对象存储 HOT	弹性IP	Web应用防火墙(边缘云 断) NEW
大数据/AI	GPU云主机	云硬盘 HOT	云间高速	Web应用防火墙 HOT
本 全 帝 昂	物理机	云主机备份	VPN连接	服务器安全卫士 HOT
	弹性高性能计算	云硬盘备份	NAT网关	Anti-DDoS流量清洗
应用产品	函数计算	弹性文件服务	对等连接	渗透测试
甄选应用	大興云県面HOT	云存储内关	虚拟私有云	SSL VPN
省份专享	大英云电脑 HOT	云版房置访 NEW	共享市员 HUT	域名无忧
	弹性伸缩服务	AT19 000	内网DNS	网页防篡改
	镜像服务	CDN	弹性负载均衡	日志审计
		下载加速	VPC终端节点	DDoS高防IP
	专属云	全站加速 NEW	云专线CDA	数据加密
	安尾云 (计算独享型)	安全加速 NEW	天翼云SD-WAN	密钥管理 NEW
	专属云 (存储独享型)	静态加速	SSL VPN	叙加库安 <u>生</u> 终端本来
	专属云容器引擎	视频直播	今世中间代	· 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2.
	专属云分布式满息服务 Kafka	视频点播加速	TE TE 44 Ind 4	微隔案防火爆
	专属云(关系型数据库	视频监控 NEW	分布式消息服务	云下一代防火墙
	MySQL)	云点播	分布式消息服务RocketMQ	无辱垒机

步骤2. 点击<立即开通>,跳转购买页面。

○ 天翼云	最新活动	产品	解决方案	云网融合	宠价	应用商城	合作伙伴	支持与服务	了解天襄云				Q	中国站~
			ļ	弹性云主机 CPU、内砾、 可服安全的时	云主 (CT-ECS, 策隆, 云 算环境, : 算环境, :	机 Elastic Clou 硬盘组成,同 确保服务持久I 計算職 〉	d Server) 是 时塔合VPC、 稳定运行。	—————————————————————————————————————	、 弹性 可扩展的计 副本保存等能力,	算服务。云主机由 打造—个 倾 高效又				
				产品类型		产品优势	产	品功能	应用场景	服务案例	视频教程	使用帮助	相关产品推	存
				促销活动						重要通知				
				免费试用 () 最新活动 2 代惠活动 1 (代惠活动 1	本验新—代 云领智企, 自购专场, E机爆款钼	注机, 20+款; 1C2G云主机(精选主机,产品 潮, 1C1G云;	云产品,最长 低至86元/年, ,首购74元/4 主机低至88元	免费1年 领1.84万元助力 F起 /年	金	· 通知 关于 · 通知 网站 · 通知 关于 · 通知 【安	线上发票申请入口开放的通 安全检测产品下线通知 因系统维护 暂停提供发票的 全通告】 Linux Polkit 权限	動的 的通知 是升漏洞风脸通告(CVE	-2021-4034)	

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
		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。
		● 包年/包月
01	计费模式	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	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。
		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。
09	安全组	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。
		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。
10	弹性公网 IP	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,若部署环境中有 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。

Bit Bit Recomplete relationship Refer Refer Bit B	рияналан (О. и 1800 1800	88886 Q 86/8768 () 45	2000 स. साथ-प्रावस . स्वाध्यप्रवस. • 00 • 7.07 ±25 •	202 • 	Ent I用分区
NUMBER NUMBER NUMBER NUMBER NUMBER NUMBER NUMBER NUMBER NUMBER NUMBER	яражее () 20, 30,	898895 Q Mar/arthr () 18	000534. TAL/READEL BELORES. 92 0 • 737 235 •	不用区域的完成品件 第400-500-64 第400-500-64 第400-500-64 第 利用区1 可用区2 医 医 第 第 1	用分区
RHG2 RHG2 <th< th=""><th>арекие () 30. 30.</th><th>初時年年 (2) 秋水 / 広大市坂 (2) (日</th><th>92 (0) • एतम</th><th>可用E2 医 単純系列 ・ vCPUs 全部</th><th>用分区</th></th<>	арекие () 30. 30.	初時年年 (2) 秋水 / 広大市坂 (2) (日	92 (0) • एतम	可用E2 医 単純系列 ・ vCPUs 全部	用分区
BEREFI VCML EB PMP EB RRBAR Q ANDO BEREFIX RVML BEREFIX Q INTER RVML RVML RVML RVML INTER RVML RVML RVML RVML <th>АРКИТИ 0 ИЛЛИНИ 30</th> <th>初巻名称 Q 私意 / 伝大物版 ① 4日</th> <th> 内存 全部 VIDIB型 </th> <th></th> <th></th>	АРКИТИ 0 ИЛЛИНИ 30	初巻名称 Q 私意 / 伝大物版 ① 4日	 内存 全部 VIDIB型 		
Bit RAT COVIA ABIT TATHSON CALL RESEARCH CALL BITE BITE TATHSON CALL DATE	рияки: 3 1	規約24作 Q. 振渡 / 職大物強 ⑦ JE	▼ 内部 全部 ▼	最新系列 + vCPUs 全部	
地理 通常計算編集 内容化は のべいと無当 総数化を のべいと無当 総プレート 数点 (単大学家 ③ 注声 は加減1 15/01/1 (16) 0.09/13/02/10 1 は加減1 15/01/1 (16) 0.09/13/02/10 1 は加減1 15/01/1 (46) 0.09/13/02/10 1 15/01/1 (46) 0.05/13/02/10 1 1 15/01/1 (46) 0.12/15/02/10 1 1 15/01/1 (46) 0.12/15/02/10 1 1 15/01/1 (46) 0.21/15/02/10 1 1 15/01/1 (46) 0.21/15/02/10 1 1 15/01/1 (46) 0.21/15/02/10 1 1 15/01/1 (46) 0.21/15/02/10 1 1 15/01/1 (46) 0.21/15/02/10 1 1	204988285 30 31	基点/最大物版 ⑦ JΞ	15 million and 10 million		5
NBRX/P VCM1 MP (CM), IE NE / 8 XM (8 XM (% CM), IE i slamuk1 1xCM0 1.GR 0.66 / 83.0 kb; i slamuk1 1xCM0 2.GR 0.66 / 83.0 kb; i slamuk1 1xCM0 4.GR 0.66 / 83.0 kb; i slamuk2 2xCM0 4.GR 0.12 / 45.0 kb; i slamuk2 2xCM0 4.GR 0.23 / 1.0 kb; i slamuk2 4xCM0 16.GR 0.23 / 1.0 kb; i slamuk2 4xCM0 16.GR 0.23 / 1.0 kb;	19688218 (1) 30 30	基度 / 最大带宽 ⑦ JΞ		通用型 通用计算增强型 内存优化型	
s3.matl.1 1xCh5,11 GB 0.06 / 0.3 GB/n s3.matl.m.2 1xCh5,12 GB 0.86 / 0.3 GB/n s3.matl.m.2 1xCh5,12 GB 0.86 / 0.3 GB/n s3.matl.m.4 1xCh5,14 GB 0.86 / 0.3 GB/n is3.matl.m.4 1xCh5,14 GB 0.86 / 0.3 GB/n is3.matl.m.4 1xCh5,14 GB 0.12 / 0.3 GB/n is3.mage.4 2xCh5,14 GB 0.12 / 0.3 GB/n is3.mage.4 2xCh5,14 GB 0.25 / 1.60 /s is3.mage.4 4xCh5,14 GB 0.25 / 1.60 /s	3		vCPUs I 内存(GiB) JΞ	按检名称	
s skimedum2 hCr0s j 2.68 0.66 / 63.6824 d medum4 hCr0s j 4.68 0.57 / 35.6824 Ø stalage4 2.6704 j 4.68 0.12 / 85.6824 Stalage4 2.6704 j 4.68 0.12 / 85.6824 Stalage4 2.6704 j 4.68 0.12 / 85.6824 Stalage4 2.6704 j 4.68 0.12 / 55.6824 Stalage4 4.6704 j 16.68 0.25 / 1.6045	3	0.05 / 0.3 Gbit/s	1vCPUs 1 GIB	s3.small.1	
s3medium.4 hcfbis / 4 G8 666 / 63 Calits Ø bliege 2 hcfbis / 4 G8 612 / 83 Galits s1 stage 4 hcfbis / 4 G8 612 / 83 Galits stalsge 4 hcfbis / 8 G8 612 / 63 Galits stalsge 2 hcfbis / 8 G8 625 / 1 Galits stalsge 4 hcfbis / 16 G8 625 / 1 Galits		0.06 / 0.3 Gbit/s	1vCPUs 2 GIB	s3.medium.2	
(b) 31.6gg 2 3xXP05 (4 G8 0.12 / 0.5 G80;5 c) slauge 4 3xXP05 (8 G8 0.12 / 0.5 G80;5 s).slauge 2 4xXP05 (8 G8 0.25 / 1.60;5 s).slauge 4 4xXP05 (15 G8 0.25 / 1.60;5	3	0.06 / 0.3 Gbit/s	1vCPUs 4 GIB	S3.medium.4	
slutge4 3xx70x 6 G8 0.12 / 0.5 Gbth slutge2 4x00x 8 G8 0.25 / 1 Gbths slutge4 4x00x 16 G8 0.25 / 1 Gbths	60	0.12 / 0.5 Gbit/s	2vCPUs 4 GIB	s3.large.2	
st.slage2 4x70s 6.68 0.25 / 1.65x5 st.slage4 4x70s 16.68 0.25 / 1.65x5	60	0.12 / 0.5 GbR/s	2vCPUs 8 GiB	S3.large.4	
S3.slarge.4 44CP05 [16.GB 0.25 / 1.Gb0(s	94	0.25 / 1 Gbit/s	4vCPUs 8 GIB	S3.xlarge.2	
	9	0.25 / 1 Gbit/s	4vCPUs 16 GiB	S3.xlarge.4	
S3.2xHarge.2 8vCPUs 16 GIB 0.5 / 1.5 Gbit/s	12	0.5 / 1.5 Gbit/s	8vCPUs 16 GIB	S3.2xlarge.2	
当时的语 通用型 (+3.)arge-2.1 2vCPUs (+4.GIB				当前规括 週用型 s3.large.2 2vCPUs 4 GiB	

系统盘	普通IO	v	-	100	+	GIB	IOPS上限700,	IOPS <u>突发上限</u> 2,200	
	 培加一块数据盘 您还 	可以挂载 23	块磁盘	(云硬盘)				

购买包年/包月云主机时添加的非共享盘磁盘不支持单独退订和续费,非共享的数据盘不支持挂载到其他云主机。

网络 扩服网卡	vpc-default (192168.0.0/16) ・ 如果希望新術者が成功表示 ※可参加2000年64日 ② 加加の一時用令 地区可以加加	C subnet-default (192.168.0.0/24) •	C 自动分配P地址	 ・ ・ ・	
¢⊉il	 〒WAF (c252a64a-9993-49f4-b4f9-ff9976c) 安全出映総防火策功能、風一个接張上的分組、 降酸全全接列約 へ 入方向規則 出方向規則 	18983) • • C 新聞堂会祖 ⑦ 用于设置网络访问经制。			
	安全组名称	INVINCE ①	供型	2001 () 2001 ()	描述
		TCP: 22	IPv4	0.0.0.0	
		TCP; 4431	IPv4	0.0.0.0/0	
	-	TCP: 80	IPv4	0.0.0.0/0	
	ZWAF	TCP: 443	IPv4	0.0.0.0/0	

云主机名称	ecs-6a61 购买多台云主机时,名称目动按序增加4位数字后编	。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	密码 密钥对	创建后设置	
用户名	root		
密码	请妥善管理密码,系统无法获取您设置的密码内容。		
确认密码	请再次输入密码		
云主机组 (可选)	反亲和性 ⑦ 请选择云主机组 查看云主机组	• C	
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。

			搜索 Q 筹	9物车 备实 管理控制台 帮助中心
最新活动 📧 📌 品 🗸 解决方案 🗸	定价 开放云市场 ~ 合作伙伴 ~	开发者。 服务与支持。 关于移动云。 乡村振兴		
查看所有产品 >	○ 请输入产品各称			
推荐产品 >	弹性计算	云存储	云网络	云安全
House B	云主机 ECS	对象存储 EOS	虚拟私有云	云安全中心
<u>esau/~on</u>	GPU云主机 GACS	云硬盘 EBS	弹性公网IP	抗DDoS服务
大数据	FPGA云主机 FACS	云空间	共享带宽	增强震调扫描
	导种性伸缩 EAS	云存储网关 CSG	NAT网关	漏洞扫描
九天人工智能	裸金屬服务醫 BMS	文件存储 EFS	弹性负载均衡	云主机安全
	容離服务 KCS	云硬盘督份 BBS	IPSec VPN	Web应用防护
物联网	物联网 容器镜像服务 CIS		SSL VPN	态势感知
en=	云主机备份 CBS	并行文件存储 PFS	对等连接	云堡垒机
1424	撓像服务 IMS	云聲俗	IPv6转换	容器安全
移动云A系列产品	专屋宿主机 DDH	云归档	云端口	DDoS辘防
	VMware专属云 VMDC	云醫份CBR	云互联	Web金线防护
	函数计算 SFC	混合云容灾	云专线	数据加密
	Linux系统订阅服务 CLS		5G云梯(公测中)	密钥管理
	云虞南	管理与监控	大云云盒	网页防要改
	云手机	云监控	云解析	数据库审计
	云电脑 NEW	ZAPI	全局流量管理	日志進行
		云電計 Audit	VPC终端节点	敏感数据保护
	数据库	云日志	内网DNS NEW	云下一代防火塘

步骤2. 点击<立即订购>, 跳转购买页面。

© the star	搜索	Q <u>购物年</u>	箭突	管理控制台	幕肋中心
最新活动,1991 产品。解决方案。定价开放云市场。合作伙伴,开发者。服务与支持,关于移动云。乡村服兴					
云主机 ECS 云主机 ECS (Dataic Compute Server)是一种检测环境的 二級服务器,为定提供原可象,例性扩展 的计算资源差别。受可以根据需求是非不可提供的 二級服务 一般 量件 5% 点 一般 量料 网络 半級銀合 的注意 14 、 風記的 竹木化 战务 常来、 云王明 从 了 预算 计 新研 的 一般 电低 计规 可 市 物 能 通 企 版 印 文服 1 图 文服 1 图					
了解更多: 价格详细 帮助中心 价格计算器					
【最新活动】 云主机免费试用30天! 100					
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
		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。
		● 按年计费
		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。
01	计费模式 	● 按月计费
		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。
		● 按时计费
		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。
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。
		部署云 WAF 选择 x86 计算架构。
		● x86 计算
03	架构	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。
04	公米	不同类型的主机适用的场景不同。
04		部署云 WAF 选择通用性即可。
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
		● 安全加固
		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。 部署云 WAF 天此要求,免费赠送可开启。
		即有云 WAI 九此安尔,尤贝ォ达马力力。
07	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。
		前者云 WAF 建议系统温 100G 以上。
08	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。 网卡选择默认网卡即可。
		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。
09	公网 IP	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,若部署环境中有 NAT 网关等,根据实际环境进行调整。
		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。
10	安全组	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。
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	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。
		昨日日 110 马 51低油 5 你 同 儿 能 直 此 为 能 , 臣 马 个 能 直。

费方式	按	年计费	按月计费	按时计费	0							
	按时计器	会在每个月底	复篮想的使用情况给	您提供话里, 需要提前	『充值。							
92	华中卡	长沙2	~	可用区1	0							
	不同地域移动云各	的实例之间内的资源池命名全的	9 旦不相通;远择露 新改版,若您对新旧	近您的地域,可降低M 资源池命名关系存在第	外格时廷、提高您的访问 部8,可查看资源池名和	小速度 尔新旧版映射表						
(7)												
191												
S	x8	6 计算										
* 0		5 (FR 70)	·秦田四後/6/1/刑	市営停ル帯	由海田地(平)(中)	\$2+++++ 5 4再	1180	21.首四+6	(+) (V#I	12 56 + 12 10	+ 801世刊)面中103-62-6878-FE
~•		8/046	100/10 Million Concession	131710/044	PSHTPSHIDURUA	BANTE	11	11 AMS	UUHUGE	BRIKE	~8082	10/10/14 14 15 14
6	全部vC	CPU规格		全部内存规格	~ 接	名称搜索						
		10101		相构勾约	(四)副日(十%		CBLI(187)	rb#(CD)	5776tr #*		金融价格(二小小小	
		X01HBX			CF0重号/主领		VCF0(88)	PMP(GB)	Page to	(96Hc/)(GDI(/S)	8-5011B()(/)(b)	
		通用型		s1.medium.2	Intel Xeon Gold	5118@2.3GHz	1	2	0.5		0.19070//Jv#g	_
		通用型		s1.medium.4	Intel Xeon Gold	5118@2.3GHz	1	4	0.5		0.320元/小时	- 1
		通用型		s1.large.1	Intel Xeon Gold	5118@2.3GHz	2	2	1		0.350元/小时	
	0	通用型		s1.large.2	Intel Xeon Gold	5118@2.3GHz	2	4	1		0.390元/小时	
		通用型		s1.large.4	Intel Xeon Gold	5118@2.3GHz	2	8	1		0.500元/小时	
^{远择实例} 竟像	s1.large	ə.2 2CPU 4G内	存 1Gbit/s									
^{新选择实例} 镜像	sl.large	5.2 2CPU 4G内	存1Gbit/s				10					
^{前选择实例} 镜像 镜像来源	sl.large	5.2 2CPU 46/5	存 IGbit/s 公共镜像	*	公有镜像	共享镜	چ	镜像市	汤	<mark>▼</mark> 安	·全加固 ⑦	
^{前近梁实例} 镜像来源	sl.large	5.2 2CPU 4GP	存1Gbit/s 公共镜像	ŧ	公有镜像	共享境	像	镜像市	汤	<mark>⊻</mark> 安	全加固 ⑦	
^{新运得实例} 镜像 镜像来源	sl.large	5.2 2CPU 46/5	存1Gbit/s 公共镜像 mtOS	5	∆有镜像 ~ (共享镜 CentOS 7.9 6	像 4/立	镜像市	汤	<mark>▼</mark> 安	全加固 ⑦	
^{能选择实例} 镜像 镜像来源	sllarge	22 2 CPU 464	存1Gbit/s 公共镜像 intOS	ž	∆有镜像 ── (共享镜 CentOS 7.9 6-	優 4位	镜像市	ž	<mark>⊻</mark> 安	全加固 ⑦	
^{新选择实例} 镜像来源	sl.large	Ce	存 IGbit/s 公共镜像 mtOS	8	∆有镜像	共享镜 CentOS 7.9 6-	優 4位	镜像市	汤	2 安	全加固 ⑦	
^{此近将实列} 镜像来源	sllarge	Ce	存 IGbit/s 公共镜像 ntOS	*	∆有镜像 ~ 〔(共享镜 CentOS 7.9 6	像 4位	镜像市	5 <u>5</u>	☑ 安	全加固 ③	
镜像。	sl.large	.2 2СРU 4GP	存 IGbit/s 公共镜像 mtOS	*	∆有镜像	共享境 CentOS 7.9 6	後 4位	镜像市	5 5	2 安	全加固 ⑦	
^{前武勇实例} 镜像 镜像来源 存储	sllarge		存 IGbit/s 公共镜像 mtOS	*	∆有镜像	共享境 CentOS 7.9 6	優 4位	镜像市	3	2 安	全加固 ⑦	
^{前选接实例} 镜像 镜像来源 存储 系统盘	sllarge	22 2CPU 46/5	存 IGbit/s 公共镜像 ntOS	*	∆有镜像	共享镜 CentOS 7.9 6	像 4位	- 镜像市 	汤 100	2 安	全加固 ③	
^{前选得实例} 镜像 镜像来源 存储 系统盘	stlarge	22 2CPU 46P	存 IGbit/s 公共镜像 ntOS	*	∆有镜像 ~ 〔 ~ 【	共享镜 CentOS 7.9 6 生能优化型	· 集 4位	镜像市: ~	题 100	⊻ 安	全加固 ⑦	
^{総通報案例} 镜像 镜像來源 存储 系统盘	stlarge	×2 2 CPU 464 CE 元、	P IGBH/s 公共镜像 mtOS 硬盘	*	△有镜像	共享镜 CentOS 7.9 6 生能优化型 褒盘性能指标	·像 4位	镜像市 ~	නි 100	⊻ 安	全加固 ⑦	
^{前选得实例} 镜像 镜像来源 存储 系统盘	stlarge	22 2 2 CPU 4 G 4	F IGBH/s C A C A C A C A C A C	#能指标不同, 话 () (推荐开	ム有镜像 	共享镜 CentOS 7.9 6 生能优化型 硬盘性能指标	像 4位	镜像市 ~ ~ ~	题	⊻ 安	全加固 ⑦ ☆ GB	
(mittifieren) 镜像 镜像来源 存储 系统盘	stlarge	22 2 CPU 464 C E 元 不同 利用	F IGBH/s C A C A C A C A C A C A C C A C	* 能指标不同, 访 (推荐开 路定期针对2	ム有镜像 → (共享 , , , , , , , , , , , , ,	像 4位 	镜像市	汤 100 了解更多	⊻ 安	全加固 ⑦ ☆ GB	
#15.9440) 镜像 镜像来源 存储 系统盘	stlarge	22 2 CPU 464 C C E 不同 利用	ア IGBN	* 上能指标不同。 - (分 (推荐开 分务定期针对 2	ム有镜像	共享 第 CentOS 7.9 6 生能 优 化型 夏 曲 生 能 优 化 型 夏 曲 仕 能 指 标 不 の の の の の の の の の の の の の	像 4位 杀、数据景	镜像市	汤 100 了解更多	⊻ 安	全加固 ⑦	
 前选得实例 镜像 镜像来源 请像来源 存储 系统盘 数据盘 	stlarge	22 2 CPU 464 C C E 不同 利用 您巴	ア IGBN	* 能指标不同, · (分 (推荐于 分定期针对2 器盘,还可以)	ム有镜像 → (→ 1 <u> 査若</u> 各美云 日 日 日 日 日 の ・ 西援5 块	共享 た	像 4位 染、数据表	镜像市- ~ ~ 問等风险。	汤 100 了解更多	⊻ 安	全加固 ⑦	
#15.9 ¥ C M 镜像 镜像来源 镜像来源 石 括 系统盘 数据盘	stlarge	22 2 CPU 464 C C C 不同 利用 您已	7 IGBN	* 上能指标不同, · (分 (推荐于 3会定期针对2 器盘,还可以试	ム有镜像 → (→ 1 <u> 査若</u> 各类云 日 日 一 一 日 一 一 一 一 一 一 一 一 一 一 一 一 一	共享 第 CentOS 7.9 6 生能优化型 現血性能指标 以応対病毒感	像 4位 交 数据表	镜像市 ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	汤 100 了解更多	⊻ 安	全加固 ⑦	

* 网络	建现机有云
	vpc_default > subnet_default(2409.8c50.fff > C 可用标声问数量253个
	如现有些拟私有云/子网不符合物的要求,可以去拉制台 新建进料私有 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	按属定带宽计器 按使用流量计器
接入类型	弹性公网IP
	弹性公网PIT取从关闭80、8080、443、8443端口,如需使用,请您先进行ICP备套,备套通过后为您开造上述端口!
* 带宽	0 hbps
	语手动属整带觉,就认OMbps为不开通带觉,最大规格为500Mbps,如率订购更大带觉,语愿过 工单申请,
安全组	重新法律な全組
	为国外認太王制的安全性。那時時物改王計團KASA時间LIX第正1001用日理理堂處。如何 開建了(加長基) 如果認識要近程的问题的云主机,请确保此安全絕升放特定論曰(Linux產并放Z2論口)、Windows產并放389期口)。如何 配置? 其他问题 ?
* 登录党业	
*登录密码	清输入
*确认密码	
	请午口恐怖设置的密码,如远远可登录ECS定制台里宣密码,者不填远密码对了自定又密码,则载认为的建后用设置 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。
* 空侧夕称	ECS-70007232
X01H0	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	不超过100个字符
高级洗顶	云主和自会义数据
194X297X	
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。 你是会可以沿费10个标本,沿等的标签将应用在本次创建的所有可以
	10 NOV 10 NOVE 10 1 NOVE 1 OCENTRY AND NOVEMAN AND NOVEMAN PARTY NOVEMAN PARTY NOVEMAN AND NOVE

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。

🎭 联通云		请输入您	想搜索的关键词(2、 文档 控制台
品 ~ 解决方案 ~	云市场 服务与支持 ~ 合作	15生态 关于联通云	资讯	
	Q. 搜索云产品			
	计算	存储	网络	应用服务
云安全	云服务器 ECS HOT	云硬盘 BSS	专有网络 VPC	消息队列 Kafki
开发与运维	裸金属服务器 BMS	对象存储 OSS HOT	负载均衡 SLB	GIS引擎
	GPU 云服务器	云硬盘备份 VBS	弹性公网IP EIP	孔雀大屏
边缘计算	弹性伸缩 AS	文件存储 NAS	NAT网关	统一鉴权
十物堤片人下起能	镜像服务 IMS	蓝光存储 BRD	云间高速 ECN	报表引擎
	专属专区 DZ	云服务器备份 CSB	内网DNS	灵云CMP
IoT物联网		云存储网关 CSG	共享带宽	
	数据库			
	云数据库 RDS MySQL版	视频与CDN	容器服务	
		内容分发网络CDN	容器服务 CSK	
	云或加声 RDS PostgreSQL 版	视频监控	弹性容器实例 ECI	

步骤2. 点击<立即购买>, 跳转购买页面。



序号	参数	说明
		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。
		● 包年/包月
01	付费类型	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。

步骤3. 购买ECS服务器, 配置购买服务器参数

		部署云 WAF 选择 x86 计算架构。
		● x86 计算
03	架构	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。
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。
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。
		部者云 WAF 选择公共镜像-Cent OS-Cent OS 7.9 64bit
		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。
06	系统盘	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。
07	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。
		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。
08	安全组	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。
09	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 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
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

		散地创建在不同的主机上,提高业务的可靠性。 部署云 WAF 可以根据实际情况勾选或不勾选此功能。
13	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。
14	专属宿主机	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。 部署云 WAF 可以根据实际情况配置此功能,也可不配置。
15	购买数量	根据实际需求选择购买云服务器的数量。

付费类型:	包年包月 按量计	践						
云区域/专区	厦门一区 ∨ 不同云区域的云产品之间内网不互通。	通用专区2 请教师还将算近您让男的云区域,可减少同	通用专区1 18时段,细胞访问速度。					
架构	x866±10							
规格	通用型 内存型	网络增强型 本地存储型						
	現格名称	VCPU	内存	处理器型导	处理器主须/参须	内网带宽	内网收发包	
	s1.medium1	1vCPU	1GB	Intel Gold 5120	2.2 GHz/3.2 GHz	1 Gbps	2435 PPS	÷
	s1.medium2	1vCPU	ZGB	Intel Gold 5120	2.2 GHz/3.2 GHz	1 Gbps	2437 PPS	
	s1.medium4	1vCPU	4GB	Intel Gold 5120	2.2 GHz/3.2 GHz	1 Gbps	2475 PPS	
	s1.large2	2vCPUs	ZGB	Intel Gold 5120	2.2 GHz/3.2 GHz	1 Gbps	24万 PPS	- 1
	s1.large4	2vCPUs	4GB	Intel Gold 5120	2.2 GHz/3.2 GHz	1 Gbps	24万 PPS	
	S1.large8	2vCPUs	8G8	Intel Gold 5120	2.2 GHz/3.2 GHz	1 Gbps	2437 PPS	
	S1.xlarge4	4vCPUs	4GB	Intel Gold 5120	2.2 GHz/3.2 GHz	1 Gbps	2435 PPS	
	S1.xlarge8	4vCPUs	8GB	Intel Gold 5120	2.2 GHz/3.2 GHz	1 Gbps	24万 PPS	*

镜像		常用镜像	公共鏡像	私有镜像								
		CentOS	v	CentOS 7.9 64位	V							
系统盘		SSD云盘		✓ 50G 免费赠道	ŧ.							
数据盘	Θ	SSD云盘		v] [-] [70 + 0	B 可选范围	: 10-32768GB	数量	-	1	+	
	۲	增加一块数据盘您送 购买包年/包月云	还可以挂载7块菱 8务器时添加的	牧掘盘 数据盘不支持单独线	5. 典							
专有网络VPC	vpc_xiamen(192.168 1子同(192.168.1.0/2 如果蜀夏其他专有网络	aans) > で 4) > で 目初が WPC, 線光絵園や有月線VPC 文	▲配和同Pv4地址 ∨ 軍需要與他子网,请先该通	- 1791								
选择安全组	云WAF 安全祖美術的火燒功能	 〇 創建安 1. 是一个逻辑上的分组、用于设置 	b组 网络访问控制。									

入方向規則(5) 出方向規則(2)				
terox	登録	980	接权对象	
TCP	ipv4	443-443	0/444.0	^
TCP	ipu4	80-80	0/4440	
TCP	ipv4	4431-4431	0/00.0	
ICMP	ipu4	不限制满口	0(0.0.0.0	
TCP	ipu4	22-22	0/0.0.0	~

弹性公网IP	 現在购买 (使用已有 为每台云股份器分配法享的IP-44 	 · 暫不法導 · · ·			
带宽计器方式	按固定等宽				
带宽大小	O 1M	О 200М	 600M	0- 800M	0 - 1 Hbps

实例名称	₩AF	
登陆方式	密码 密钥对	
登录名	root	
登录密码	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
确认密码		
云服务器组	开启反亲和性 ⑦	
资源组	默认资源组 🗸 🔾	
专属宿主机	请选择专属宿主机 ∨ ③ 创建专属宿主机	
购买数量	- 1 + 台 您最多可以创建 50台云服务器	

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。

w 加 庙田 CENITO	c 7	
Metch Cento	570	
您在安装过程中想使用『	那种语言?	
Slovenčina	Slovak	简体中文 (中国)
Slovenščina	Slovenian	繁體中文 (台灣)
Shqip	Albanian	繁體中文 (中華人民共和國香港特別行政區
Српски	Serbian	简体中文 (新加坡)
Svenska	Swedish	
தமிழ்	Tamil	
తెలుగు	Telugu	
Точикй	Tajik	
ไทย	Thai	
Türkçe	Turkish	
Українська	Ukrainian	
اردو	Urdu	
Tiếng Việt	Vietnamese	
中文	Chinese 🗲	
IsiZulu	Zulu	
在这里进行搜索。	Ø	

步骤3. 配置Cent OS 7的安装信息摘要。

	安装信息摘要				CENTOS 7 安装	[
					🖽 cn	帮助!
CentOS	本地化					
Reply III	\odot	日期和时间(T) 亚洲/上海 时区		键盘(K) 汉语		
Bask	á	语言支持(L) 简体中文 (中国)				
4.15 1. 1.	软件					
	0	安装源(I) 本地介质	6	软件选择(S) 基础设施服务器		
	系统					
	S	安装位置(D) <i>已选择自定义分区</i>	Q	KDUMP 已后用 Kdump		
	< →	网络和主机名(N) 未连接		SECURITY POLIC No profile selecte	c Y d	
		۲				
					退出(Q)	开始安装(B)
				在点击开始安赛	官按钮前我们并不会	操作您的磁盘。

- 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。

手动分区			the set of the set		CENTOS	7 安装
完成(D)					🖽 cn	帮助!
▼新 CentOS 7 安装			centos-swap			
数据 /data	k	80 CiP	挂载点(P):	设备	r:	
centos-data		80 GIB				
/home centos-home		5116 MiB	期望容量(D):	Virti	o Block Device (vda)	
系统			5120 MiB			
/boot vdal		5120 MiB				
/var centos-var		15 GiB		16	纪2(M)	
/ centos-root		10 GiB	设备类型(T):	Volu	ume Group	
swap		5120 MiB >	LVM -	加密(E) ce	ntos	(0 B 空闲) ▼
tentos-swap			文件系统(Y):	10	ē改…(M)	
			swap 👻	重新格式化(0)		
				A7 20	- / h h h	
			校 32 (上) .	12 MU SW	ap	
						更新设置(U)
- C				注意:在	您点击主菜单上的开始安	被按钮之前,您
2010 日2210					任本屏幕内所做的设置更	且成不会被应用。
92.5 KiB 120 Gi	iB					
选择 1 个存储设备(S)						全部重设(R)
anu エクリカ(-N) 成(D) ■ 以太网 (ens18)					centros 7	菜 助!
Intel Corporation 82540EM	G	正在编辑	ens18 (on localhost)			关闭
	连接名称(N): ensl	.8				
	常规 以太网	802.1X 安全性	DCB Proxy	IPv4 设置 IPv	6 设置	
	方法(M): 手动				-	
	the bi-					
	地址	子网掩码	网关		Add	
	10. 3.57	255.255.0.0	10. 255.2	54 mi	除(口)	
		[·				
	DNS 服务器:	114.114.114.114				
	搜索域(E):					
	DHCP 客户端 ID:					
	需要 IPv4 地址	完成这个连接				
				路日	3(R)	
-						配置(0)
			10	Cancel	保存(S)	
(H) : localhost.loc	caldomain	应用(/	A)		当前主机	记名: localhost



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。

	配置	CEN c	TOS 7 安装 n 帮助!
CentOS	用户设置		
Nersellin.	ROOT 密码 已经设置 root 密码	● 创建用户(U) 不会创建任何用户	
Filmen			
de same			N
	● 正在安装 kernel (336/485)		
	CentOS Virtualization SIG Virtualization in CentOS, virtualization of CentOS wiki.centos.org/SpecialInterestGroup		

步骤6. 安装完成后重启系统即可完成安装。

CentOS	配置 用户设置	CEN Boot	ITOS 7 安装 :n	帮助!
	COT 密码 已经设置 root 密码	创建用户(U) 不会创建任何用户		
R. BRAN				
	完成!	 CentOS	日成功安装并可	
		centos		友(R) 言(R)
	A 使用本产品即表示遵守此许可协议 /usr/share/centos-release/EULA			

3.3. 安装云 WAF

云WAF安装包列表如一	F	:
-------------	---	---

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。

🐺 Choose which file(s) to ι	ipload			>
\leftrightarrow \rightarrow \land \frown	> 此电脑 > 软件 (D:) > WAF8.0.60	~ C .	〇 搜索"WAF8.0.60"	
组织 ▼ 新建文件夹			∎ • ∎	•
> 🗾 视频	~ 名称	修改日期	类型	大小
> 🔀 图片	WAF8.0.60_20220415.pkg	2022/4/19 14:49	PKG 文件	1,642
> 📑 文档	WAF8.0.60_dependency_20220415.pkg	2022/4/19 14:35	PKG 文件	137,3
→ 🛓 下载	Constraint and supervised	2022/4/19 14:34	ZIP 压缩文件	2,7
> 🕜 音乐 💦 👔		2022/4/15 17:10	Microsoft Word	6,7
> 🥅 桌面		2022/4/15 17:14	Microsoft Word	6
> ៉ 系统 (C:)		2022/4/14 10:49	Microsoft Power	13,1
>		2022/4/19 10:22	Microsoft Word	10,5
文件名	<u>N</u>): WAF8.0.60_20220415.pkg			~
			打开(2) 取	消

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.
<pre>[root@waf-fefcfe40384a tmp]# setenforce 0 setenforce: SELinux is disabled</pre>
<pre># 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</pre>

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 _rwx-rxr_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。

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。

Dependencies Resolved	cmpj# ./#xP8.0.00_dependent	y_zozzowistpkg -one die			
Package	Arch	Version	Size		
Installing: docker-ce	×86_64	20.10.10-3.e	L7 23M		
Package Summary					
Install 1 Dependent pack Is this ok [y/N]: y	kages				
三加製器件,「おはStating」 正在整査ではおいまでも、 このれまが時では、いう、4、1133、 正在整査、のはない、4、200、11 正在整査、docker-ce-101、 正在整査、docker-ce-101、2010、10. 正在整査、docker-ce-101、2010、10. 正在整査、docker-ce-101、2010、10. 正在整査、docker-ce-101、2010、10. 工作者は、大切を大型の、10. 二、工作者素のない、10. 二、数件他、docker-ce-10. 、2011、2011、2011、2011、2011、2011、2011、201	r, langpacks .4.11.3.1.47.806.64.rpm; .4.17.806.64.rpm; 不要研己 .1.05.3.67.806.64.rpm; .05.3.67.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.rpm; .20.10.10.3.617.806.64.0.200 .00.10.10.10.10.3.617.1880 .00.10.10.10.10.10.10.10.10.1880 .00.10.10.10.10.10.10.10.1880 .00.10.10.10.10.18.807.1880 .00.10.10.10.1880 .00.10.10.1880 .00.10.10.1880 .00.10.1880 .00.10.1880 .00.18800 .00.18800 .00.18800 .00.18800 .00.18800 .00.18800 .00.18800 .00.18800 .00.18800 .00.18800 .00.18800 .00.188000 .00.188000 .00.18800000	containerd.10-1.4.11-3.1. 英語教授书品。 ckerr.ce.20.10.10-3.e17.xi 1:docker.ce.21.20.10.10 変能教育件の。 x86 64.rpm: docker.ce.ror x86 64.rpm: docker.ce.ror m 将受支援 1: docker.scan-plugin-0.9 支援会教件名。 1: docker.scan-plugin-0.9 支援会教件名。 1: docker.scan-plugin-0.9 支援会教件名。	बो7, x88_64 16_64 3.el7, x86_64 tisse-extras-20.10.10-3.el7, x88_64 0-3.el7, x85_64		
Package		·····································	版本		
而在成绩。					
docker-ce		x86 64	3:20.10.10-3.el7	/docker-ce-20.10.10-3.el7.x86 64	96 M
docker-ce-rootless-ext		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 cless Transaction test Succees Running transaction 正在安装 : docker- 監证中 : 3:docke 新证中 : 3:docke	:k ded -ce-20.10.10-3.el7.x86_64 :e-rootless-extras-20.10.11 :e-rootless-extras-20.10.11 -ce-20.10.3.el7.x86_64)-3.el7.x86_64 -3.el7.x86_64			1/2 2/2 1/2 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	grepcolor=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-fefcfe40384ă tmp]# chmod +x WAF8.0.60_20220415.pkg [root@waf-fefcfe40384a tmp]# ll 送用量 1779488 drwx----- 3 root root 17 4月 8 14:45 systemd-private-2b0f49b859da489c8ce2bc96566126c3-chronyd.service-dUJX5j -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



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: Netscape Comment: OpenSSL Generated Certificate X509v3 Subject Key Identifier: 09:51:39:55:96:85:05:95:16: 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: $\downarrow ~\uparrow ~\rightarrow ~\leftarrow ~$ and / toggles search Select Deployment Method Plugin ----- Selected Deployment Method Reverse Proxy 216.5MB/216.5MB 181.4MB/181.4MB 150kB/150kB 52.85MB/52.85MB 218.9MB/1.077GB Mgent Management Platform Configurations 7.0.0.1:4431 Platform in Plantom + Management Plantom Configurations
int Plantom + Management Plantom + Managem 1m3AA:xx,1 12WL12notRN6w+kmyPJVFt0xe 39Wj59JA86t9017C203+jE93Z Xx1KIHsm35yUmtsmF1icvEbSl 4g+GzuJ411RD+7lJJt3Gp/sX 4g+GzuJ411RD+7lJJt3Gp/sX 4g+GzuJ411RD+7lJJt3Gp/sX 4g+GzuJ411RD+7lJJt3Gp/sX 4g+GzuJ411RD+7lJJt3Gp/sX 4g+GzuJ411RD+7lJJt3Gp/sX 4g+GzuJ411RD+7lJJt3Gp/sX 4g+GzuJ411RD+7lJt3Gp/sX 4g+Gzu h5104gH3nSwsR9WnxLGRpkgFECGkBZ0EUwrbF GDzj70kAaiCflH+LjWToY+CJtl19ev10cg/1pz bnn/&8KkoDipPhoBNYga6x+CQKPkEJCnkiTCBF слявстотакулонародски от элих и то ракатину баркизанту зукра кененару на самарикание самарикание самарикание с макатикание и праводски по славит на самарикание самарикание самарикание самарикание самарикание самарикание с на праводскати праводска на самарикание самарикание самарикание самарикание самарикание самарикание самарикание tallation Configurations Command: monitor info nt Platform URL:<u>https://127.0.0.1</u>:4431 ll WAF Success Gwaf-fefcfe40384a tmp]# 📕

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_nginx、waf_detect四个容器正在运行。

列出所有在运行的容器信息: dokcer ps

列出本地镜像: docker images



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。

		~		
← → ヾ ↑ └└	> ID电脑 > 软件 (D:) > WAF8.0.60	<u> </u>	2	
组织 ▼ 新建文件夹				
> 🚺 视频	名称 ^	修改日期	类型	大小
> 🔀 图片	WAF8.0.60_20220415.pkg	2022/4/19 14:49	PKG 文件	1,642
> 🗧 文档	WAF8.0.60_dependency_20220415.pkg	2022/4/19 14:35	PKG 文件	137,3
> 🛓 下载		2022/4/19 14:34	ZIP 压缩文件	2,7
> 🕜 音乐 💦 👔	Contraction in the second second	2022/4/15 17:10	Microsoft Word	6,7
> 🎫 桌面		2022/4/15 17:14	Microsoft Word	6
> ៉ 系统 (C:)		2022/4/14 10:49	Microsoft Power	13,1
> 🚍 软件 (D:)		2022/4/19 10:22	Microsoft Word	10,5
文件	培(N): WAF8.0.60_20220415.pkg			~
		ſ	±T∰(O) III	3 E

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。



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]



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。

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]# . Dependencies Resolved	ot&waf-fefcfe40384 tmp]# ./WAF8.0.60_dependency_20220415.pkg -online endencies Rasolved					
Package	Arch	Version	Size			
Installing: docker-ce	x86_64	20.10.10-3.el7	23М			
Package Summary						
Install 1 Dependent packages Is this ok [y/N]: y						
1ntilling pstage docker: Distanting pstage docker: Distanting the starting of the starting	upgata 2 3.117.805 64.rpm: Container 605 64.rpm, 不更新ご変化的な。 13.105,805 64.rpm 13.105 65 64.rpm 13.105 65 75 75 75 75 75 75 75 75 75 75 75 75 75	L io -1, 4, 11-3. 1, el7, x80_64 E : 10.10-3. el7, x80_64 e-cl.1 > 20, 10, 10-3. el7, x80_64 docker.ce.roolless-extras-20, un-plugin-0.9. o-3. el7, x80_64 考査。 7. 神敏 変統	19.10-3.417.x86_64			
Package	架构	版本		*	大小	
正在安装: docker-ce docker-ce-rootless-extras	x86_64 x86_64	3:20.10 20.10.1	.10-3.el7 0-3.el7	/docker-ce-20.10.10-3.el7.x86_64 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64	96 M 20 M	
事务概要 						
安装 2 軟件包 总计,116 M 安装大心;116 M Downloading packages; Running transaction check Running transaction test Transaction test succeeded Running transaction 正在安装 : 3:dober-ce-c2	0.10.10-3.e17.x86.64				1/2	
验证中 : docker-ce-root 验证中 : 3:docker-ce-26	less-extras-20.10.10-3.el7.x86 0.10.10-3.el7.x86_64	64			1/2 2/2	

步骤5. 安装完成后,执行docker ps查看docker是否运行

[root@waf-fe	fcfe40384	la tmp]# doc	ker ps				
CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	5	NAMES
[root@waf-fe	fcfe40384	la tmp]# doc	ker images				
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE			
[root@waf-fe	fcfe40384	la tmp]# ps	-aux grep	docker			
root 80	23 0.0	1.5 1163304	60152 ?	Ssl	15:44	0:00	/usr/bin/dockerd -H fd://containerd=/run/containerd/containerd.sock
root 212	31 0.0	0.0 112728	972 pts/0	R+	16:16	0:00	grepcolor=auto docker
[root@waf-fe	fcfe40384	la 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 [root@waf-fefcfe40384a 总用量 1779488	tmp]# chmod +x ' tmp]# ll	WAF8.0.60	_20220415.pkg
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
- FWYF-YF-Y 1 Foot Foot	140664202 4 8	10 15.22	WAES 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

步骤8. 选择需要部署模式为 (插件), 回车确认。

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: dokcer ps

列出本地镜像: docker images



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_procésses auto;
error_log /var/log/nginx/error.log notice;
              /var/run/nginx.pid
load_module /etc/nginx/ngx_1.21.6_http_waf_agent_module.so;
events {
    worker_connections 1024;
http {
    include /etc/nginx/mime.types;
default_type application/octet-stream;
     include
    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。



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:

#custor	n 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。

Choose which file(s) t	o upload			
÷ → ~ ↑ [┣ > 此电脑 > 软件 (D:) > WAF8.0.60	~ C .	户 搜索"WAF8.0.60"	
组织 🔻 新建文件夹			∎ • ∎	
> 🚺 视频	名称 ^	修改日期	类型	大小
> 🔀 图片	WAF8.0.60_20220415.pkg	2022/4/19 14:49	PKG 文件	1,642
> 📲 文档	WAF8.0.60_dependency_20220415.pkg	2022/4/19 14:35	PKG 文件	137,3
> 🛓 下载	Concernant sectors of	2022/4/19 14:34	ZIP 压缩文件	2,7
> 🚺 音乐 💦 👔		2022/4/15 17:10	Microsoft Word	6,7
> 🧱 桌面		2022/4/15 17:14	Microsoft Word	e
> 造 系统 (C:)		2022/4/14 10:49	Microsoft Power	13,1
> 🚍 软件 (D:)		2022/4/19 10:22	Microsoft Word	10,5
			i	
文件	笔(N): WAF8.0.60_20220415.pkg			
		ſ	打开(2) 取	消

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。



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]# chm [root@waf-fefcfe40384a tmp]# ll 台田書 137369	od +x	WAF8.0.60	_dependency_20220415.pkg
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。

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]# Dependencies Resolved	./WAF8.0.60_dependency_202204	15.pkg -online			
Package	Arch	Version	Size		
Installing: docker-ce	×86_64	20.10.10-3.el7	23M		
Package Summary					
Install 1 Dependent packages Is this ok [y/N]: y					
Installing package docker: Installing package docker: 正在地路重。constant do.1.4.1 containerd.to.1.4.113.1.e17 正在地路重。constant do.1.4.1 containerd.to.1.4.113.1.e17 正在地路重。docker.ce.113.0.15 正在地路重。docker.ce.113.0.15 正在地路重。docker.ce.113.0.15 正在地路重。docker.ce.113.0.15 正在地路重。docker.ce.113.0.15 正在地路重。docker.ce.115 正在地路重。docker.ce.15 正在地路重要。file docker.ce.rootle 	angpake 2.5.1.el7.x86.64.rpm: containe x86.04.rpm, 不里房已要能的低 2.1.s.el7.x86.04.rpm: iidskir x86.94.rpm, 新聞已要能的低 2.1.s.el7.x86.04.rpm: iidskir x86.94.rpm, 不服已受整的低 2.0.s.el7.x86.04.rpm, iidskir y86.04.rpm, 不是那已要能的低 7.x80.04.rpm, 不是那已要能的低 5.2.01.01.0-3.07.%86 ss-extras.x86.64.0.20.10.10-3.1	rd.io-1.4.11-3.1.el7.x86_64 生む。 20.10.10-3.el7.x86_64 -ce-cli-20.10.10-3.el7.x86 -ce-cli-20.10.10-3.el7.x86 -co-cli-20.10.10-3.el7.x86 -co-cli-20.00-3.el7.x86 -分配。 -co-cli-20.00-3.el7.x86 -分配。 -20.7 将彼 安装	9 64 95-20.10.10-3.617.x86_64 16_54		
Package	架构	ħ	反本	<i>ж</i>	大小
正在安装: docker-ce docker-ce-rootless-extras	x86_64 x86_64	3 2	::20.10.10-3.el7 0.10.10-3.el7	/docker-ce-20.10.10-3.el7.x86_64 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64	96 M 20 M
事务概要					
安装 2 软件包					ľ
总计: 116 M 安装大小: 116 M Downloading packages: Running transaction check Running transaction test Transaction test <u>succeeded</u> Running transaction 正在安装 : 3:docker-ce-ro 脸证中 : docker-ce-ro 脸证中 : docker-ce-ro 脸证中 : 3:docker-ce-ro	20.10.10-3.el7.x86_64 stless-extras-20.10.10-3.el7.x stless-extras-20.10.10-3.el7.x p10 10:3.217.v86.44	36_64 36_64			1/2 2/2 1/2 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 1163394 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

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-fefcfe40384ā tmp]# chmod +x WAF8.0.66_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 WAF8.0.66_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



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



c377c28a3e43: Load	ing layer	[======================================	52.85MB/52.85MB
914120db83a9: Load	ing layer	[======================================	1.077GB/1.077GB
8d1dc0b00b3f: Load	ing layer	[======================================	13.82kB/13.82kB
360f6aa95169: Load	ing layer	[======================================	2.264MB/2.264MB
a93f4df02f78: Load	ing layer	[======================================	434.2kB/434.2kB
17fc118b9866: Load	ing layer	[======================================	5.632kB/5.632kB
e311caf2fa28: Load	ing layer	[======================================	4.096kB/4.096kB
ab2eb94ebe5e: Load	ing layer	[======>]	327MB/440.3MB
ALLEY CLASSING ALL STREET			

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: dokcer ps

列出本地镜像: docker images



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,并上传云WAF软件依赖安装包与安装包到/tmp目录下。

Choose which file(s) to	upload			×
$\leftrightarrow \rightarrow \sim \uparrow$	→ 此电脑 → 软件 (D:) → WAF8.0.60	~ C	^D 搜索"WAF8.0.60"	
组织 ▼ 新建文件夹			∎ - ∎	1 2
> 🗾 视频	名称 ^	修改日期	类型	大小
> 🔀 图片	WAF8.0.60_20220415.pkg	2022/4/19 14:49	PKG 文件	1,642
> 📲 文档	💾 WAF8.0.60_dependency_20220415.pkg	2022/4/19 14:35	PKG 文件	137,3
> 🛓 下载		2022/4/19 14:34	ZIP 压缩文件	2,7
> 🕜 音乐 💦 👔		2022/4/15 17:10	Microsoft Word	6,7
> 🧾 桌面		2022/4/15 17:14	Microsoft Word	6
>, 🏪 系统 (C:)		2022/4/14 10:49	Microsoft Power	13,1
> 🚍 软件 (D:)		2022/4/19 10:22	Microsoft Word	10,5
文件名	۲ <u>(N):</u> WAF8.0.60_20220415.pkg			
			打开(2) 取	ji j

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-fefcfe40384a tmp]# setenforce 0 setenforce: SELinux is disabled
<pre># 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. # sELINUXTYPE=targeted</pre>

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 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。

<u>▲</u>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]# Dependencies Resolved	./WAF8.0.60_dependency_202204	15.pkg -online			
Package	Arch	Version	Size		
Installing: docker-ce	x86_64	20.10.10-3.el7	23М		
Package Summary					
Install 1 Dependent packages Is this ok [y/N]: y					
netalling package dokkri 正在業項 回転期間, 1944 11-3.1.e47.386 64.rpm: Containerd.io-1.4.1-3.1.e47.486_064 grantmard soil.1413.1.a1.0.rpm 有法律意 doktrice-roil.201.1013.617.886 64.rpm 刊述gate 1.doker-ce.102.0.10.10-3.e17.486_064 doktrice-roil.201.1013.617.886 64.rpm 刊述gate 1.doker-ce.102.0.10.10.3.e17.486_064 moder-ce-roil.201.1013.617.886 64.rpm 刊述gate 1.doker-ce.102.0.10.10.3.e17.486_064 doker-ce-roil.201.1013.617.886 64.rpm 刊述gate 1.doker-ce.102.0.10.10.3.e17.486 Doker-ce-roil.201.1013.617.886 64.rpm 刊述gate 4.doker-ce.100.0.101.0.3.e17.486 Doker-ce-roil.201.1013.617.886 64.rpm 刊述gate 4.doker-ce.100.0.101.3.e17.486_064 doker-ce-roil.201.1013.617.886 64.rpm 刊述gate 4.doker-ce.1000.0.1013.617.886_064 doker-ce-roil.201.1013.617.886 64.rpm 刊述gate 4.doker-ce.1013.886 64.0.001.0.10.3.e17.486 64 doker-ce-roil.201.1013.886 64.0.201.0.10.3.e17.486 64 doker-ce-roil.201.1013.886 64.0.201.0.10.3.e17.486 64 doker-ce-roil.201.1013.886 64.0.201.0.10.3.e17.486 64 doker-ce-roil.201.1013.886 64.0.201.0.10.3.e17.486 64 doker-ce-roil.201.1013.886 64.0.201.0.10.3.e17.486 64 doker-ce-roil.201.1013.886 64.0.201.0.10.3.e17.486 64 doker-ce-roil.201.101					
Package	架构	版本		源	大小
正在安装: docker-ce docker-ce-rootless-extras	x86_64 x86_64	3:20. 20.10	10.10-3.el7 0.10-3.el7	/docker-ce-20.10.10-3.el7.x86_64 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64	96 M 20 M
事务板要 					
安装 2 秋件也 总计: 116 M 安装大小: 116 M Downloading packages: Running transaction check Running transaction test Transaction test succeeded Running transaction Transaction	10 10 -2 +17 ×96 64				
正在安装 : docker-ce-roo 验证中 : docker-ce-roo 验证中 : 3:docker-ce-20	tless-extras-20.10.10-3.el7.x tless-extras-20.10.10-3.el7.x 5.10.10-3.el7.x86_64	36_64 86_64			2/2 1/2 2/2

步骤15. 安装完成后,执行docker ps查看docker是否运行



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 [root@waf-fefcfe40384a 总用量 1779488	tmp]# chmod +x tmp]# ll	WAF8.0.60_20220415.pkg
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

8O#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]



步骤18. 确认部署角色后,输入管理节点的IP,端口(默认为20001),管理节点的证书和Token回车即可安装。



步骤19. 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检测节点会有waf_nginx、waf_detect两个容器正在运行。

列出所有在运行的容器信息: dokcer ps

列出本地镜像: docker images



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。

-	🚞 > 此电脑 > 软件 (D:) > WAF8.0.60	~ C	〇 搜索"WAF8.0.60"	
1织 🔻 新建文件夹			∎ - ∎	1
🛃 视频	名称 ^	修改日期	类型	大小
🔀 图片	WAF8.0.60_20220415.pkg	2022/4/19 14:49	PKG 文件	1,64
📱 文档	WAF8.0.60_dependency_20220415.pkg	2022/4/19 14:35	PKG 文件	137,
业 下载		2022/4/19 14:34	ZIP 压缩文件	2,7
🕜 音乐		2022/4/15 17:10	Microsoft Word	6,
🧱 桌面		2022/4/15 17:14	Microsoft Word	
- 🏪 系统 (C:)		2022/4/14 10:49	Microsoft Power	13,
🚍 软件 (D:)		2022/4/19 10:22	Microsoft Word	10,
文	牛名(N): WAF8.0.60 20220415.pkg			Ŵ

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.
# SELI	NUX= 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.
SELINU	IX=disabled
# SELI	NUXTYPE= 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.
SELINU	IXTYPE=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]



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]# Dependencies Resolved	./WAF8.0.60_dependency_2022	20415.pkg -online			
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: 二式教授書「Asternations and Asternations and Asternations and Asternations and Asternations and Asternational Asternational Asternation and Asternational Asternational Asternation and Asternational Ast	angpack 1 - 30.64 / 1 - 30.7 / 30.64 / 1 - 50.7 / 30.64 / 1 - 50.5 /	inerd.io-1.4.11-3.1.el7.x86 故告題。 なら見し、10-3.el7.x80_64 err-ce-cl20.10.10-3.el7.x8 が行き。 1.rpm: そのためにてee-rootless-ex 文字 err-scan-plugin-0.9.0-3.el7. 対数件也。 -3.el7 特徴 安装	64 6_64 Tras-20.10.10-3.el7.x06_54 888_64		
Package	架构]	版本	*	大小
正在安裝: docker-ce docker-ce-rootless-extras	×86_ ×86_	64 64	3:20.10.10-3.el7 20.10.10-3.el7	/docker-ce-20.10.10-3.el7.x86_64 /docker-ce-rootless-extras-20.10.10-3.el7.x86_64	96 M 20 M
●方依安 → → → → → → → → → → → → →					
文献 されてき 会計: 115 M 安藤大小, 116 M 安藤大小, 116 M pownloading packages: Running transaction check Running transaction test Transaction test succeeded Running transaction 正在安装 : 3:docker-ce-ro 融近中 : 3:docker-ce-ro 融近中 : 3:docker-ce-ro 融近中 : 3:docker-ce-ro	20.10.10-3.el7.x86_64 otless-extras-20.10.10-3.el7 otless-extras-20.10.10-3.el7 0.10.10-3.el7.x86_64	′.x86_04 .x86_64			1/2 2/2 1/2 2/2

步骤5. 安装完成后,执行docker ps查看docker是否运行

[root@war-tetcte40384a 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	6:16 0:00	grepcolor=auto docker
Front@unf fofcfo/020/n tmn]#			

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 [root@waf-fefcfe40384a 总用量 1779488	tmp]# chmod +x tmp]# ll	WAF8.0.60	20220415.pkg
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
-rwyr-yr-y 1 root root	140664292 4 日	10 15:33	WAE8 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



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
```

vrite out database with 1 new entries	
Data Base Updated	
Deployment Method: Plugin	
2653d992f4ef: Loading layer [====================================	======] 216.5MB/216.5ME
f1affad69343: Loading layer [====================================	=====>] 181.4MB/181.4ME
18a6d2a77388: Loading layer [====================================	======================================
:377c28a3e43: Loading layer [====================================	======] 52.85MB/52.85ME
014120db83a9: Loading layer [====================================	=======] 1.077GB/1.077GE
3d1dc0b00b3f: Loading layer [====================================	======================================
360f6aa95169: Loading layer [====================================	======] 2.264MB/2.264MB
a93f4df02f78: Loading layer [====================================	======================================
17fc118b9866: Loading layer [====================================	======================================
311caf2fa28: Loading layer [====================================	=====>] 4.096kB/4.096kB
ab2eb94ebe5e: Loading layer [====================================	=======] 440.3MB/440.3ME
11d23d2c1f83: Loading layer [====================================	======================================
62b40fdf1aa3: Loading layer [====================================	======] 2.189MB/2.189ME
0268ba6f0efd: Loading layer [====================================	=====>] 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: dokcer ps

列出本地镜像: docker images



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,并上传云WAF软件依赖安装包与安装包到/tmp目录下。
$\leftrightarrow \rightarrow \checkmark \uparrow$	→ 此电脑 > 软件 (D:) > WAF8.0.60	~ C	の ター 搜索"WAF8.0.60"	
			∎ - ∎	
> 🔝 视频	名称 ^	修改日期		大小
> 🔀 图片	WAF8.0.60_20220415.pkg	2022/4/19 14:49	PKG 文件	1,642
> 📲 文档	WAF8.0.60_dependency_20220415.pkg	2022/4/19 14:35	PKG 文件	137,3
> 🛓 下载		2022/4/19 14:34	ZIP 压缩文件	2,7
> 🕖 音乐 👘	and the second second second	2022/4/15 17:10	Microsoft Word	6,7
> 🥅 桌面		2022/4/15 17:14	Microsoft Word	e
> ៉ 系统 (C:)		2022/4/14 10:49	Microsoft Power	13,
> 🚍 软件 (D:)		2022/4/19 10:22	Microsoft Word	10,5
文作	丰名(N): WAF8.0.60_20220415.pkg			

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.
# mli - 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 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。

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 t Dependencies Resolved	mp]# ./WAF8.0.60_dependency_202	20415.pkg -online				
Package	Arch	Version	Size			
Installing: docker-ce	×86_64	20.10.10-3.el7	23M			
Package Summary						
Install 1 Dependent pack Is this ok [y/N]: y	ages					
三加載編集, Fatssmirred, io-1 三加載編集, Fatssmirred, io-1 containerd, io-1,4,13,3,1 三世信息業 docker-co-10,10 正定性意業 docker-co-10,20 正定性意業 docker-co-10,20,10,0-3 正定性意業 docker-co-10,20,10,0-3 正定性意素 docker-co-10,20,10,0-3 正在性意業 docker-co-10,20,10,0-3 正在性意業 docker-co-10,20,10,0-3 正在性意業 docker-co-10,20,10,0-3 正在性意業 docker-co-10,20,10,0-3 正在性意業 docker-co-10,20,10,0-3 二、数件性自 docker-co-10,20,20,20,20,20,20,20,20,20,20,20,20,20	「」 Langeskis - (Langeskis - (Lins, Lai)、 - (Lins, Fargesel 2, Lins, Lins, Fargesel 2, Lins,	inerd.io-1.4.11-3.1.el7 数件包. ce-20:10.10-3.el7.x86_6 ker-ce-cli-20.10.10-3.e %(件包. 4.rpm: docker-ce-rootle 支援 をでき がい件包. -3.el7 将彼 安装	.x86_64 4 17.x86_64 seatras-20.10.10-3.el7.x86_64 .el7.x86_64			
Package		aຢ	版本			大小
正在安装: docker-ce docker-ce-rootless-extr	×86 as ×86	64 64	3:20.10.10-3.el7 20.10.10-3.el7	/docker-ce-20.10.10-3.el7.x86_ /docker-ce-rootless-extras-20	64 10.10-3.el7.x86_64	96 M 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 chest Transaction test Succeed Running transaction 正在安装 : 3:docker- 证在安装 : docker-c 验证中 : docker-c 验证中 : docker-c	k ed e-cool.10.10-3.el7.x86_64 e-rootless-extras-20.10.10-3.el e-rootless-extras-20.10.10-3.el re-20.10.10.21.27.86.64.el	7.x96_64 7.x96_64				1/2 2/2 1/2 2/2

步骤15. 安装完成后,执行docker ps查看docker是否运行

[root@waf	-fefcf	e40384	1a tmp]# doc	ker ps				
CONTAINER	ID	IMAGE	COMMAND	CREATED	STATUS	PORT	S	NAMES
[root@waf	-fefcf	e40384	1a tmp]# doc	ker images				
REPOSITOR	Υ ΤΑ		IMAGE ID	CREATED	SIZE			
[root@waf	-fefcf	e40384	1a 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	grepcolor=auto docker
[root@waf	-fefcf	e40384	1a 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 [root@waf-fefcfe40384a 总用量 1779488	tmp]# chmod +x tmp]# ll	WAF8.0.60_20220415.pkg
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
many and a dimension and	140664202 4	to triad little o co dependency apagoits also

步骤17. 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WAF Agent(检测节点),回车确 认。

cd /tmp

./ [云WAF安装包名]



步骤18. 确认部署角色后,输入管理节点的IP,端口(默认为20001),管理节点的证书和Token回车即可安装。



步骤19. 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检测节点会有waf_detect这个容器正在运行。

列出所有在运行的容器信息: dokcer ps

列出本地镜像: docker images

rootewaf-fefcfe92b045 tmp]# docker ps OMFAINER ID IM46E Ambdicam8015 W af_detect:8.0.60.321B */bin/sh -c 'chmod +_" 47 seconds ago Up 45 seconds 0.0.0.0.6970-6971->6970-6971/tcp, :::6970-6971->6970-6971/tcp waf_detect

步骤20. 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;
nid /var/run/nginx.pid:
load_module /etc/nginx/ngx_1.21.6_http_waf_agent_module.so;
events {
    worker connections 1024;
http {
    include /etc/nginx/mime.types;
default_type application/octet-stream;
     include
    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。



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:

#custor	n 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<u>https://管理节点IP:4431</u>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>。

← → C ▲ 不安全 https://10. 3.57:4431		ŝ	£≞	9	<u>\</u>
	你的连接不是专用连接				
	な曲者可能试測从 10				
	NET:ERR_CERT_AUTHORITY_INVALID				
[陸臨市政				
	此服务器无法证明它是 10.243.3.57:你的计算机的操作系统不信任它的安全证书。这可能 是由错误配置或者有攻击者截获你的连接而导致的。				
[继续访问 10. 1.57 (不安全)				



贴合业务 持续对抗	第46日日22 第46日日22 日日 愛 企業咨询	
保护混合多云时代的每一个数字化应用	深信服WEB应用防火墙	
	Réé	
API	新聞入田戸谷 ♥ 	
APP		
111	1479年144日20日 山田子 一 我已用約井同倉 用户使用协议 路私政 策	
	立即登录	

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。

G 深信服WAF	监控 安全防护 节点管理 日志管理 系统管理
系统管理	
拉制台参数	邮件服务器系统时间 授权管理 隐私设置
	设备基础信言
⑦ 安全能力更新	援权状态 ● 未授权 援权数活动间 -
0 +m======	2012 使用在132211 使用VIS221212521212532122532323233332332 使用在1322222 使用在13222222 使用在13222222 使用化132222 使用化132222 使用化132222 使用化132222 使用化132222 使用化132222 使用化13222 使用化132222 使用化13222 (用化13222 使用化13222 (用化13222 (用化132222 (用化132222 (用化13222 (用
🛆 管理员账号	振行 1
88 系统维护 >	
0	安全功能模块开通及安全能力升级序列号
	1882/2018-7712/32/2019-22-2018-08/05-2019-2110-38-010- - 安全功能序列号
	状態の 大振家 大振家 大振家 应用于保障业务系统的安全、主要包括WEED印刷的护等 通过主动能征的方式、记录的问答是正常用户还是机器
	功能 流量,对制度流量进行有效功许,留神业务安全。 摄权有效时间:- 摄权有效时间:-
6	云前、丁间服务,序列号 用版业务需求并否约回约、丁间服务
	大路、大路に新聞かめ規則は古り4個勝方 特性的方金生成力进行行現。 化超「Webの運動防御集」 海辺立時後江20時時時期則率,保持改革用就检測的機量 新規則的能力
	唐代有效时间:-
•	软件升级
	软件升级 味熱(2) 施収空冷系統软件版本的更新升级 操权电效时间:

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。

控制台参数	邮件服务器系统时间 授权管理 隐私设置	
	设备基础信息	
	接权状态 💿 已授权	接权激苦时间 2022-06-14
	授权类型 在线接权(试用版) 更新授权 切换至VLS授权服务器授权	授权用户
	授权吞吐 ① 200M/s	网关序号 B871EF3B
	援权ID T25E2-86F8-6268-	援权序列号 9861-3176-CB79-
	接权节点数 ① 并1个,已接权1个	
0	安全功能模块开通及安全能力升级序列号 根据业务需求开启对应的安全功能模块以及安全能力更新升级功能	
	• 安全功能序列号	
	● 医疗物的小的能开通 应用于保障业务系统的安全,主要包括WEB应用的护等 为能 差常可要的时间。2022-07-14	■ ■ 2000 広式, 记别的问者是正常用户还是机器 显出于有效防护, 保障业务安全。 2022-07-14
6	云端订闻服务序列号	
	根理业务需求开启对应约订阅服务 云鏡、云台局新藏納防御规则库订阅服务 把领权支全部方进行升税、包括"Web应用防护库"、调 调应式特征证用库等规则库"、保持设备具备检测的如量 新成款的能力 提仅有效时间:2022-07-14	
٢	软件升级	
	软件升级 接受支持系统软件被本的面新升级 接受有效控制间:2022-07-14	

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。

⑦ 深信服WAF	曲拉 安全防护 节 <u>点管理</u> 日志管理 系统管理	⑦ 🧶 admir
节点管理		
节点列表 <1	waf-10.243.3.88 。正常	
	1月20년 10.243.3.88 内存 4G8 CPU 2C 谜盘 117.008	10./17月 2022-04-21 14-20-07 夏安在各称 2022-04-21 14-20-07
	系的なる 检測状态 告留日志 と1小打 - 熟練时间每隔: 1000	C
	CPUEBR No. No.<	ち ち ち ち ち ち ち ち ち ち ち ち ち ち ち ち ち ち
<u>д18</u> с 1 л Э	 <	200/10/06/18 Copie 20 00 00 00 00 00 00 00 00 00

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。

深信服WAF	监控 安全防护 节点就理 日志管理 系统管理	🕐 🥌 admin
节点管理		
节点列表(waf-10.243.3.87 * 正第	
Bitte Bitter Q	IP#31上 10.243.3.87 内存 4G8	加入时间 2022-04-21 16:10:46
💿 • waf-10.243.3.87 🜖	CPU 2C 把型 117.0GB	最近更新时间 2022-04-21 16:10:46 更改名称
📄 • waf-10.243.3.88 🏮	取続れる 社際状态 田原日志 ① <u> </u> <u> </u>	c
	CPUBR#	Image: constraint of the second sec
R28, (] /)	磁盘体用字 % 70 73 23	Xiz/tet/sina * WIDRE

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。

新城	8	启用	熱用	Bile .			全部健康状态 ×	•	全部WEB防护策略	×	全部BOT防护策略 ×	站点名称/城名/监	听她口		C
	序号	健康状态	6	站在名称	防护城名	服务类型		监听第日	1	WEB防护策略	BOT防护策略	启用/禁用	摄作		
	1	正常		门户网站	10. 57	http		80	1	WEB防护策略	BOT防护策略		编辑	展制	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)。

节点池											
名称:	云WAF检测节点池										
/用述: 节点选择策略:	请剩入/面还信息 哈希			~ (0						
按优先级调度:		● 禁用									
哈希字段:	SRC_IP			~							
节点:	IP 輸入域名、IPv4/IPv6地址或用"-"连			接的IP	范围		靖口:	输入端口		0	[] 添加
选择节点:	× 删除										
	类型	IP地址	端口			权重		优先级		操作	
	IP	10.243.3.87	80			÷				编辑	删除
	IP	10.243.3.88	80							编辑	删除
健康检查	当前已配置 2 会记录										
健康检查方法:	已选择(1/5) 💿		日新	*		待选 (38)			C	清榆	λQ
	connect_tcp				« »	TCP被动 ping ping6 connect_ http ftp pop3	udp				
	节点有效条件: 常規	险查方法 全部		•							
	节点恢复方法:	手动恢复	討恢复	3			分钟	~	0		

<u>▲</u>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。

3称:	适传客户端IP		
苗述:	请输入描述信息		
TTP缓存			
HTTP缓存:	○启用	● 禁用	
TTP压缩			
HTTP压缩:	○启用	●禁用	
Ë			
适传IP到服务器:	○ 启用	○禁用	
传输类型:	传输客户端IP至原	后台服务器	•
HTTP头部名称:	X-Forwarded-For		

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。

拟服务					
基本信息					
名称:	云WAF负载策略				
描述:	请输入描述信息				
启/禁用:	● 启用	○ 禁用			
服务类型:	НТТР			~	
IP地址:	192.168.1.23				
端口范围:	80				
入口链路:	● 所有链路	○指定链路			
默认节点池:	云WAF检测节点池	B	~	1 新增	
SNAT策略:	自动SNAT			~	,
源端口策略:	保持			~	•
	🔹 隐藏以下配置				

HTTP优化策略:	适传客户端IP	*	📑 新増
HTTP2策略:	NONE	~	<mark>1</mark> 新增
TCP策略:	NONE	•	📑 新増
安全策略			
HTTP防护策略:	NONE	×	📑 新増
	NONE		1+ xc+m

🛄 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。
------	--------------------------------

深信服WAF	监控 安全防护 节点管理 系统管理		🕐 🧧 admin
节点管理			
节点列表	l waf-10.243.3.87 ●正常		
·····································) IP158년 10.243.3.87 P3위# 4GB	版入时间 2022-04-21 16:10:46 用at-dx-67	
📄 🔹 waf-10.243.3.87 🏮	CPU 2C 磁盘 117.0GB	最近更新时间 2022-04-21 16:10:46	
📄 • waf-10.243.3.88 🕥	新修成 注意的状态 音音日志・● 近日小村・・・ 第8時日前日 100		C
	CPUERI# 10 73 23 24 25	内存使用車 第 100 75 50 23 ペント 二一一一一	
	0 1 MARINA MARA - CARACTER 1540 1550 1600 1610 1620 1630 1640	0 1540 1550 1600 1610 1620 1630	16:40
	磁盘ゆ田李 ※	发送/接收流量 Khps ・发送元量	• 接收流量
	100	2,500	
	73	2,000	
	- 25	1,000	
共2条 (1 /1		300	

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。



🛄 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。



Web服务器

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。

⑦ 深信服WAF	监托	安全防护 1	节点管理	日志管理	系统管理	
安全防护	VEB防护策略					
G 站点防护	新增 4 1986	高级设置				
	□ 序号 策明	各名称		描述		
	- 1 🕅	人策略_业务保护场景		建议在日常运维业务保	护场最下使用,选取最准确的规则对命中的攻击进行	拦截,其余规则命中后仍
WEB防护策略 3	- 2 👯	人策略_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,提供漏洞防扫描能	力,针对恶意的漏洞扫描
BOT防护策略						
例外策略						
日 安全防护规则库	×					
♀ SSL策略						
3 黑白名单	>					
◎ 云端黑客IP防护						
*策略名称	WEB防护策略					
策略描述	唐榆λ策略描述(洗道)					
防护配置						
解析配置	✔ XML解析 ①					
云端威胁情报	✓ 云端黑客IP防护 ①					
もいいのは				会 物际 拉		
WWWWW				or search 11/		
	CSRF防护受限URL防	护山令防护了	漏洞防扫描 C	C攻击防护		
漏洞保护	• SOI(2)			· 信自洲贡功丰		
	* SQUEX		~	• 内心道路火山		· ·
	▶ 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	ŧ	~
	▶ 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	~
	ANTE - Phile		1	,后门扫描防拍		

步骤2. 在设备[安全防护/站点防护]中创建站点防护。

众 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	<1	站点防护 🌑 🛈				
I Ca 站点防护 2		新增 3 启用	禁用 翻除			
□ 策略管理	>:	序号 健康状态	3 站点名称	, ,		防护域名
6 安全防护规则库	>					
♀ SSL策略						
回 黑白名单	>.					
₲ 云端黑客IP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。
		需要防护的站点域名,支持 IP 地址和域名两种形式。 ● 填写 IP
02	防护域名	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 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。
		云 WAF 进行反向代理所监听的端口。
04	监听端口	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。
		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。
		● 加权最少连接
		表示选择(连接数/权重)最小的节点。
06	负载调度算法	● 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。
		● 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
09	保持连接方式	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。
		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。
		● 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。
11	X-Forwarded-For	● 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。
		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。
		● 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。
16	联动封锁 	● 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 令暴破防护,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	门户网站							
*防护域名	a.sangfor.com							
	添加							
*服务类型	O http	🔿 htt	ps					
*监听端口 ①	80 ×							
	輸入单个端口或端口	范围 (如:8	0-88)后,	按Enter	腱添加。最多	可以添加	16个	
备注	请输入							
法少信自								
20 A D D D D D D D D D D D D D D D D D D								
负载调度算法	○ 加权最小连接	() 源地	的此哈希	•	9轮询			
转发服务器	http 🔻 10.	3.60				:	80	×
	1	61					80	×
	nttp • 10	.01						
	http v 10							
	 http ▼ 10 添加 ✓ 启用健康检查 	设置						
保持连接方式	 nttp ▼ 10 添加 マ 启用健康检查 一切注接 		禘					
保持连接方式	 nttp ▼ 10 添加 ✓ 启用健康检查 ⑦ 短连接 默认使用长连接,请 	设置 ○ 长道 确认转发服务	接審是否支持	长连接	,若不支持,	即使设置)	5长连接,	也会使用短
保持连接方式 会话保持	 nttp ▼ 10 添加 ☑ 启用健康检查 ○ 短连接 默认使用长连接,请 ✓ 启用会话保持 	02 ● 长道 确认转发服务	接	长连接	,若不支持,	即使设置为	7长连接,	也会使用短
保持连接方式 会话保持 会话保持时间	 nttp ▼ 10 添加 ② 启用健康检查 ③ 短连接 默认使用长连接,请 ☑ 启用会话保持 1 	段置 ● 长速 确认转发服务	接 器是否支持	长连接	,若不支持,	即使设置方	5长连接,	也会使用短

头部改写	新增制				
	□ 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	暂不使用BOT防护策	略		¥	
WEB防护策略	WEB防护策略			•	展开详情
检测动作	○ 检测后放行	○ 检测后排	兰截		
联动封锁	启用联动封锁 ①				
请求检测	请求检测body大小	1024 k	(B		
响应检测	☑ 启用响应检测				
	响应检测body大小	1024 k	(B		
真实客户端IP (j)	新增	ŧ			
	□ 头部字段		IP层数	Ż	操作
			暂无数据		

步骤4. 配置完成后,点击<确定>即可完成配置。

新	8	启用	禁用	2019		全部健康状态 ×		全部WEB防护策略。		全部BOT防护第	略×	•	站应名称/b	《名/盒听测口			2	C
	序号	健康状态		站点名称	防护域名	服务类型	监听请口		WEB防护策略		BOT防护策略			启用/禁用	操作			
	1	未检测		门户网站	a.sangfor.com	http	80		WEB防护旗略		智不使用BOT策略				(R:12	2019)	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。

记录类型:	A- 将域名指向一个IPV4地址		
主机记录:	1.2.3.4.5.6	.dns-example.com	0
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 ∨	0
*记录值:	5.5.5.5		

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。

(← → 〇 ▲ 不安全 a.sangfor.com		as is is 🖞 🗐 🕌 🙁
© Live Chat 🔍 +88 01 23 564		Login Register Help
AndHost	Home V Domain V Hosting V Services V	Pages → Blog → Contact
	Powerful Web Hosting Platform!	
	Start Today	
	Scroll	
•		

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_HTTPS 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HTTPS。 用户要求对WEB的攻击行为进行安全检测和拦截,并能够发现那些IP对站点发起攻 击行为。



Web服务器

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。

密级:外部公开

深信服WAF	监控 安全防护 1 节点管	里 日志管理 系统管理	
安全防护	WEB防护策略		
G 站点防护	新增 4 調除 高级设置		
2 策略管理 2	序号 策略名称	描述	
WERDINGS 3	- 1 默认策略_业务保护场展	建议在日常运输业务保护场景下使用,选取最准确的规则对命中的攻击进行拦截,其余	x规则命中后仅i
BOTRIDE	- 2 IIC认为规格_1HTC3至10月以为380	建议在非行运物展下使用,在亚均保护安全的护叠和上,提供制制的扫描相刀,针以急	大要的/mm/出售/
個外語路			
6 安全防护规则库			
Con Languerra in 1939			
*策略名称 WE	B防护策略		
策略描述 清	<u>俞入策略描述(选填)</u>		
防护配置			
解析配置 ▼ X	MI解析 ①		
云端威肋情报 ⊻ 2	☞端羔各IP切护 ①		
协议保护	TP应用隐藏 文件上传过滤 URL防护 HTTF	异常检测 参数防护	
CS	RF防护 受限URL防护 口令防护 漏洞防扫描	笛 CC攻击防护	
漏洞保护	・ SQL注入	 ✓ ト信息泄露攻击 	,
	→ 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。

众 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	<1	SSL策略管理 证书管理 3		
G 站点防护		新進 4 武政		
品 策略管理	>	□ 序号 名称	签发时间	过期时间
6 安全防护规则库	>	- 1 默认证书	2021年10月6日 16:42:44	2031年10月4日 16:42:44
I 🛛 SSL策略 2				
■ 黑白名单	>			
C→ 云端黑客IP防护				

3称	请编入		
鄯述	请输入		
成发类型	○ 导入证书文件	○ 导入一对公私钥	
	*选择证书文件	请上传 *.pfx, *.p12 格式文件	选择
的	请输入		

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。

	WAF	监控	安全防护	1 节点管理	日志管理	系统管理	
安全防护	<i SSL策略管</i 	建 3 证书管理					
G 站点防护	新增	4 889					
62 策略管理		序号 名称			服务器证书	5	
6 安全防护规则	库 >						
♀ SSL策略 2							
■ 黑白名单	>						
 	p 請輸入名称 请输入新述(选辑) vwaf.d Ltop		~				×
* 启用协议	TLS1.0 🗹 TLS1.1	TLS1.2	TLS1.3				
□ 已选(18	/18) ①	1 I		🗌 待选(0)		搜索关键字	Q
TLS_EC	CDHE_RSA_WITH_AES_128_GCM_	SHA256					
TLS_EC	CDHE_RSA_WITH_AES_256_GCM_	SHA384					
TLS_EC	CDHE_RSA_WITH_AES_128_CBC_9	HA256					
TLS_EC	CDHE_RSA_WITH_AES_128_CBC_S	НА			×17		
TLS_EC	CDHE_RSA_WITH_AES_256_CBC_S	на					
TLS_R	SA_WITH_AES_128_GCM_SHA256		~		暫无数	E	
TLS_R	SA_WITH_AES_256_GCM_SHA384	k.					
TLS_R	SA_WITH_AES_128_CBC_SHA256						
TLS_R	SA_WITH_AES_256_CBC_SHA256						
TLS_R	SA_WITH_AES_128_CBC_SHA						
						确定	取消

步骤4. 在设备[安全防护/站点防护]中创建站点防护。

🕢 深信服WAF		监控	全防护 1 节点管理	日志管理	系统管理
安全防护	<	站点防护 🌑 🗓			
I Ga 站点防护 2		新增 3 启用 禁用	删除		
	>	序号 健康状态	站点名称	R	抗护域名
6 安全防护规则库	>				
♀ SSL策略					
回 黑白名单	>				
G 云端黑客IP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。
		需要防护的站点域名,支持 IP 地址和域名两种形式。 ● 填写 IP
02	防护域名	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 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。
		云 WAF 进行反向代理所监听的端口。
04	监听端口	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。
		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。
		● 加权最少连接
		表示选择(连接数/权重)最小的节点。
06	负载调度算法	● 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。

0.0	白田海南扒木	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。
08	后用健康位登 	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。
		● 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
09	保持连接方式	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。
		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。
		● 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。
11	X-Forwarded-For	● 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。
		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。
		● 高危行为联动封锁
16	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

		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 令暴破防护,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	门户HTTPS网站
*防护域名	vwaf. t.top
	添加
*服务类型	http Ohttps
	* SSL策略 vwaf.e t.top •
*监听端口 (i)	443 ×
	輸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	请输入
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	https • 1060 : 443
	添加
	✓ 启用健康检查 设置
*保持连接方式	
	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	在末尾追加上一跳的IP地址
头部改写	新増創除

AHCKA J	新增量				
	□ 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	暂不使用BOT防护	策略		•	
WEB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	1024	КВ		
请求检测 响应检测	请求检测body大小	1024	КВ		
请求检测 响应检测	请求检测body大小 启用响应检测	1024	КВ		
请求检测 响应检测 真实客户端IP ①	请求检测body大小 ✓ 启用响应检测 响应检测body大小 新増	1024 1024	КВ		
请求检测 响应检测 真实客户端IP ①	 请求检测body大小 ✓ 启用响应检测 响应检测body大小 新增 ● 头部字段 	1024 1024	KB KB IP,	丟数	操作
请求检测 响应检测 真实客户端IP ()	 请求检测body大小 ✓ 启用响应检测 响应检测body大小 新增 新増 头部字段 	1024 1024	KB KB IP 暫无数据	豊数	操作

步骤6. 配置完成后,点击<确定>即可完成配置。

新加		启用 第用	制除		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/监听到	9		C
	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	1	SOT防护策略	启用/禁用	操作		
	1	正常	门户HTTPS网站	a.sangfor.com	https	443		WEB防护策略		智不使用BOT策略		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。

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 ∨
	5.5.5.5	
*记录值:		

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。

	vii 10 ♥ Ŭ	
O Live Chat ↓+88 01 23 564	Login Register Help	
AndHost	Powerful Web Hosting Platform! Late Today	
	∨ Scrall	

模拟进行攻击,成功拦截,并可以查询到安全日志。

C A Ô htt

 \leftarrow

ଜ 🔻 ଓ 🌾 ଅ

					289週末可 崖巅时间	1) 70607年8880, 日禄三載 1: 2022.03.09 18:19					
安全日志 时间端 か议员	 室腔 安全防护 5 第 1 <li< th=""><th>日志管理 -09 2359</th><th>系统管理 严重等级 动作</th><th> ○ 数命○ ○ 案書 ○ 数件 ○ 前時 </th><th>详情 基础绘度 常规 时间: 方法:</th><th>2022-03-09 1819-07 GET</th><th>协议: 国旗状态码:</th><th>NTPS -</th><th>英型: 产量等级;</th><th>SQL 注入 • 中德</th><th></th></li<>	日志管理 -09 2359	系统管理 严重等级 动作	 ○ 数命○ ○ 案書 ○ 数件 ○ 前時 	详情 基础绘度 常规 时间: 方法:	2022-03-09 1819-07 GET	协议: 国旗状态码:	NTPS -	英型: 产量等级;	SQL 注入 • 中德	
(1) (学) (注) (1) (2) (3)	800 856 2022-03-09 18:19:37 2022-03-09 18:18:47 2022-03-09 18:18:44	日本98章 Web应用8330 Web应用8330 Web应用8330	 (2) 建計算量 SQL 注入 (2) 建HTTP出版页面 (2) 建HTTP出版页面 	199 200 199 200 199. 200 199. 200	动作: URL: 描述: 危需说明: 规则D: 规则名称: 参考信息: 報告在来。	担他 vvaiitop/Yid=1select user 攻击者句: select username from 攻击者利用此漂连和放流率中放过 19020047 Select语句SQL主入攻击 -	匹爾站地帶名: name from use u 編、导致WEB世纪	(]〕中HTTFS网站 rinfo where userid=1 \$佰意泄漏,他及就搞车讲户值意安;	è.		
4 5 6 7	2022-03-09 17:21:21 2022-03-09 17:21:21 2022-03-09 15:39:09 2022-03-09 15:32:16	Web@用8359 Web@用8359 Web@用8359 Web@用8359	SQL 注入 SQL 注入 过始HTTP出程页面 过读HTTP出程页面	10.2 56 10.2 .56 199.: 200 10.2 .56	深信服Wiki: 源 源IP: 源IP1回尾地: 数据包	https://sec.sangfor.com.cn/secur 199-200.5.200 美国	ity-vulnerability 源明口: XFF IP:	//detail?vuln_sfv=SF_0000_00086 54924 -	8dang=ZH-CN		T _U T _T 91
					INCLUDE EM REQUEST: GET //id=1; Host: varial Connection: sec-ch-uair Sec-ch-uair DNT: 1 Upgrade-Int User-Agent: X&hD999	ccODING TYPE-URL aspir top NA A Rand Yser 99°, "Chromium oble: 10 lations: "Windows" secure-Requests: 1 Mozillu/S0 (Windows NT 10.0; Wi	rre userid=1 H1 'v="99", "Micro n64; x64) Apple	TP/1.1 Stoft Edge",v="90" WebK0/537.36 (04TML, like Ged	so) Chrome/99.0.44 当前	844.51 Səfəri/537.36 E 序号: 1 上一亲	dg/99.0.1150.3

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。

密级:外部公开

⑦ 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 <1	WEB防护策略	
	新增 4 酬金 高级设置	
	序号 策略名称	描述
	- 1 默认策略_业务保护场景	建议在日常运维业务保护场最下使用,选取最准确的规则对命中的攻击进行拦截,其余规则命中后仅;
WEB防护策略 3	- 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,提供漏削防扫描能力,针对恶意的漏洞扫描的
BOT防护策略		
例外策略		
G 安全防护规则库 >		
② SSL策略		
■ 黑白名単 >		
。 云端黒客IP防护		
*策略名称 WEB	防护策略	
策略描述 清输	入策略描述(选填)	
防护配置		
	11 A747 0	
云端威胁情报 🔽 云道	馬馬客IP防护 ⑦	
协议保护 HTT	P应用隐藏 文件上传过滤 URL防护 HTTP	异常检测 参数防护
CSRI	防护 受限URL防护 口令防护 漏洞防扫描	CC攻击防护
浸湿厚拉		
	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	「「「「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」」」」」」」」

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。

众 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	<1	SSL策略管理	亚书管理 3					
G 站点防护		新増	4 #890					
品 策略管理	>		序号 名称	2 5	的间		过期时间	
6 安全防护规则库	>	*	1 默认证书	20.	21年10月6日 16:42:44		2031年10月4日 16:42:44	
I 🛛 SSL策略 2								
□ 黑白名单	>							
☞ 云端黑客IP防护								

名称	请编入		
苗述	请输入		
顺发类型	○ 导入证书文件	○ 导入一对公私钥	
	*选择证书文件	请上传 * .pfx * .p12 格式文件	选择
玄码	请蝓入		

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。

深信服WAF	E .,		监控	安全防护	1 节点管理	日志管理	系统管理
安全防护	<1	SSL策略管	會理 3证书	管理			
G 站点防护		新增	4 1899				
忌 策略管理	>		序号	名称		服务器证书	
G 安全防护规则库	>						
♀ SSL策略 2							
■ 黑白名单	>						
☞ 云端黑客IP防护							

尔 请输入名称		
▲ 请输入描述 (选填)		
务器证书 vwaf.al.top	•	
用协议 🗹 TLS1.0 💙 TLS1.1 🗹 TLS1.2 🔽	TLS1.3	
密算法		
□ 巳选(18/18) ①	□ 待选(0)	搜索关键字 Q
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		512
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		
TLS_RSA_WITH_AES_128_GCM_SHA256		暂无数据
TLS_RSA_WITH_AES_256_GCM_SHA384		
TLS_RSA_WITH_AES_128_CBC_SHA256		
TLS_RSA_WITH_AES_256_CBC_SHA256		

步骤4. 在设备[安全防护/站点防护]中创建站点防护。

众 深信服WAF	监持	空 安全防护	1 节点管理	日志管理	系统管理
安全防护	站点防护 🌑 🛈				
G 站点防护 2	新增 3 启目	新聞			
品 策略管理	□ 序号 @ >	康状态 站点名称		防护域	名
6 安全防护规则库	>				
♀ SSL策略					
回 黑白名单	>				
♀ 云端黑客IP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	 需要防护的站点域名,支持 IP 地址和域名两种形式。 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 本 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。 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	 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。 在末尾追加上一跳的 IP 地址 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。
	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。
		● 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。
16		● 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 令暴破防护,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	门户HTTPS网站	
*防护域名	vwaf.etop	
	添加	
*服务 类型	O http O https	
	* SSL策略 vwaf.etop ・	
<mark>*</mark> 监听端口 ①	443 ×	
	輸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	请输入	
请求信息		
<mark>*</mark> 负载调度算法	○ 加权最小连接 ○ 源地址哈希 ○ 轮询	
* 转发服务器	http • 10. 3.60 : 80	
	添加	
	☑ 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	在末尾追加上一跳的IP地址	•
头部改写	新增 删除	

.

头部改与	新增	删除			
	□ 类型	动作	参数名	参数(直操作
			暂无数据		
防护方式					
BOT防护策略	暂不使用BOT	「防护策略		20	•
WEB防护策略	WEB防护策略	Å		12	▼ 展开详情 ▼
检测动作	○ 检测后放行	○ 检测师	5拦截		
The state state		锚①			
跃动封锁					
联动封锁 请求检测	请求检测body7	大小 1024	КВ		
联动封锁 请求检测 响应检测	 」月日味如封 请求检测body⊅ ✓ 启用响应检 	大小 1024 测	КВ		
联动封锁 请求检测 响应检测	」 启用味如封 请求检测body7 ✓ 启用响应检 响应检测body7	大小 1024 測 大小 1024	КВ		
联动封锁 请求检测 响应检测 真实客户端IP ①	 □ 用用取加到 请求检测body7 ✓ 启用响应检 响应检测body7 新増 	太小 1024 測 太小 1024 翻除	КВ		
联动封锁 请求检测 响应检测 真实客户端IP()	 □ 用用取加封 请求检测body7 ✓ 启用响应检 响应检测body7 新增 ● 头部字 	大小 1024 測 大小 1024 副除 環	КВ	IP层数	操作
联动封锁 请求检测 响应检测 真实客户端IP ()	 」月日味和封 请求检测body7 ✓ 启用响应检 响应检测body7 新增 头部字 	大小 1024 測 大小 1024 動除 寝	KB KB 暂无数据	IP层数	操作

步骤6. 配置完成后,点击<确定>即可完成配置。

86		周期 第月	153		全部健康状态 ×		全部WEB防护策略 ×	•	全部BOT防护策制	8 × 💌	站总名	除/域名/监听站				C
	序号	健康状态	站点名称	防护城名	服务类型	监听纳口		WEB防护策略		BOT防护策略	A	21月/禁用	操作			
	1	正常	门户нттрs网站	a.sangfor.com	https	443		WEB防护策略		智不使用BOT策略			编辑	叙利	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。

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 ⑦
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 > ⑦
* 记录值:	5.5.5.5	

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。

e > O bu E indest/www.c cob		
○ Live Chat \ +88 01 23 564		Login Register Help
AndHost	Powerful Web Hosting Platform! Start Today	/ Bing v Contact
	∨ Sarolt	

模拟进行攻击,成功拦截,并可以查询到安全日志。

$\leftarrow \rightarrow$	C A A https://www.	.top/?id=1:select%20use	ername%20from%20us	erinfo%20where%20userid	- 1				a	* ís !) © (¢ D Ť
					×.							
					您的请求可	可能存在威胁,已被拦截						
					拦截时间	E: 2022.03.09 18:36						
	监控 安全防护	日志管理	系统管理		详情							
				_	基础信息							
安全日志				_	常规							
时间范围	0 2022-03-09 00:00-2022-03	1-09 23:59	严重等级	🗹 1000 🗹 AC	时间:	2022-03-09 18:36:03	协议: HT	TPS	世世:	SQL注入		
协议类型	🛛 🗹 http 💟 https		动作	🗹 允许 🔽 拒绝	方法:	GET #5/#	回复状态码: - 匹配以点名: 门(mHTTPS回は	严重等级:	 中危 		
9出日3					URL	vwaf. cop/?id=1;select user	name from userinfo	where userid=1				
序号	et (E)	日志英型	成約美型	週 19	描述:	攻击语句: ;select username from	u					
1	2022-03-09 18:36:03	Web.应用防护	SQL 注入	199	冠書説明: 規則D:	攻击者利用此意问监制数据集中数3 13020047	者,导致WEB亚妈相思	!酒満,這及穀獲年來 尸悟思安 至	*			
2	2022-03-09 18:19:37	Web.应用防护	SQL 注入	199	规则名称:	Select语句SQL注入攻击						
3	2022-03-09 18:18:47	Web应用防护	过滤HTTP出槽页面	199200	参考信息:							
4	2022-03-09 18:18:44	Web应用防护	过滤HTTP出槽页面	199	解决方案: 深信服Wiki:	- https://sec.sangfor.com.cn/secur	ity-vulnerability/det	ail?vuln sfv=SF 0000 000868	lang=ZH-CN			
5	2022-03-09 17:21:21	Web应用助护	SQL 注入	10.2 .56								
6	2022-03-09 17:21:21	Web应用助护	SQL 注入	10.2 .56	源 题IP:	199. 200	潮油口: 335	990				
7	2022-03-09 15:39:09	Web应用助护	过滤HTTP出槽页面	199	题IP归赠地:	美国	XFF IP: -					
8	2022-03-09 15:22:16	Web应用助护	过滤HTTP出错页面	10.2 56	数据包							TU TT 01
					INCLUDE EN	NCODING TYPE: URL						
					GET /?id=1;	select username from userinfo whe	ere userid=1 HTTP/1	.1				
					Host: vwaf.	top						
					sec-ch-ua: "	Not A;Brand";v="99", "Chromium"	"v="99", "Microsoft	Edge";v=*99*				
					sec-ch-ua-n	nobile: ?0 slatform: "Windows"						
					DNT: 1	Presente 1						
					User-Agent:	: Mozilla/5.0 (Windows NT 10.0; Wi	in64; x64) AppleWeb	Kit/537.36 (KHTML, like Geck	o) Chrome/99.0	.4844.51 Safi	ıri/537.36 Ed	g/99.0.1150.3
					添加例约				当	前序号: 1	上一条	下一条
					1							

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。

⑦ 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	WEB防护策	各					
G ALSTED	新増	4 画绘 高级设置					
	□ #5	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	则对命中的攻击进行拦击	ŝ,其余规则命中后仅i
WEB防护策略 3	- 2	默认策略_非代理访问场展		建议在非代理场景下使用	1,在业务保护安全防护基础上,	,提供漏洞防扫描能力,	. 针对恶意的漏洞扫描(
BOT防护策略							
例外策略							
G 安全防护规则库	>						
♀ SSL策略							
回 黑白名单	>						
☞ 云端黑客IP防护							
*策略名称	WEB防护策略						
策略描述	请编入策略描述 (选)	直)					
防护配置							
解析配置	XML解析 ①						
云端威肋情报 🔽	云端黑客IP防护 ①						
协议保护	HTTP应用隐藏	文件上传过滤 URL防护	户 HTTP异常检测	参数防护			
	CSRF防护 受限U	IRL防护 口令防护	漏洞防扫描 C	C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	局洞		~
	▶ 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	方护		~
	• 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。

🕢 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	站点防护 💽 🛈	
G 站点防护 2	新增 3 启用 禁用 删除	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	序号 健康状态 站点名称	防护域名
6 安全防护规则库		
② SSL策略		
回 黑白名单		
C 云端黑客IP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。 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 地址;有互联网访问需求,则填写云 WAF 宿主机 IP 地址访问需求,则均需填写。 填写域名 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。 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。

		● 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
09	保持连接方式	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。
		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。
		● 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。
11	X-Forwarded-For	● 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。
		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。 ● 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。
16	联动封锁	● 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 令暴破防护,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	门户网站				
*防护域名	a.sangfor.com				
	添加				
服务类型	O http) https			
*监听端口 ①	80 ×				
	输入单个端口或端口范	范围 (如: 80-88) 后,按Enter键添加。	最多可以添加1	6个	
备注	请输入				
请求信息					
13-3 CIENCE					
负载调度算法	○ 加权最小连接	○ 源地址哈希			
负载调度算法 转发服务器	○ 加权最小连接 http ▼ 10.	○源地址培希 ○ 轮询 3.60	:	80	×
负载调度算法)加权最小连接 http ▼ 10. : http ▼ 10. :	○源地址始希 ● 轮询 3.60 以61	:	80 80	×
* 负载调度算法	加权最小连接 http ▼ 10. i http ▼ 10. i http ▼ 10. i http ▼ 10. i	○ 源地址哈希 ● 轮询 3.60 3.62	:	80 80 80	× × ×
* 负载调度算法	 加权最小连接 http ▼ 10. http ▼ 10. http ▼ 10. http ▼ 10. 添加 	 ○ 源地址始希 ● 轮询 3.60 8.61 3.62 		80 80 80	× × ×
* 负载调度算法	 加权最小连接 http ▼ 10. http ▼ 10. http ▼ 10. http ▼ 10. 添加 ☑ 启用健康检查 设 	 ○ 源地址始希 ● 轮询 3.60 		80 80 80	× × ×
* 负载调度算法 * 转发服务器 * 保持连接方式	 加权最小连接 http ▼ 10. http ▼ 10. http ▼ 10. http ▼ 10. 添加 ✓ 启用健康检查 没 短连接 	 ○ 源地址始希 ● 轮询 3.60 4.61 3.62 2 2 ● 长连接 		80 80 80	x x x
* 负载调度算法 * 转发服务器	 加权最小连接 http ▼ 10. http ▼ 10. http ▼ 10. http ▼ 10. 添加 梁 启用健康检查 设 知连接 默认使用长连接,请确 	 ○ 源地址哈希 ● 轮询 3.60 µ.61 3.62 2 2 2 ● 长连接 ● 长连接 ● 秋连接 	::::::::::::::::::::::::::::::::::::::	80 80 80	× × ×
* 负载调度算法 * 转发服务器 * 保持连接方式 会话保持	 加权最小连接 http ▼ 10. http ▼ 10. http ▼ 10. http ▼ 10. 添加 ② 启用健康检查 设 短连接 默认使用长连接,请确 ✓ 启用会话保持 	 ○ 源地址始希 ● 轮询 3.60 µ.61 3.62 2 2 2 ● 长连接 ● 长连接 ● 长连接 	: : : : :	80 80 80	× × ×

* X-Forwarded-For	在末尾追加上一跳的IP地址		*
头部改写	新增副除		
	类型 动作 参数名	名 参数值	i 操作
	智无	数据	
防护方式			
*BOT防护策略	暂不使用BOT防护策略	•	
*WEB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 ①		
* 请求检测	请求检测body大小 1024 KB		
响应检测	☑ 启用响应检测		
	响应检测body大小 1024 KB		
真实客户端IP ()	新増制除		
	□ 头部字段	IP层数	操作
	暫无	数据	

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。

站品名称	SSL VPN
防护域名	b.sangfor.com
	添加
服务类型	• http O https
监听端口 ()	80 ×
	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	请编入
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	http * 10.2 .66 : 80
	添加
	✓ 启田健康检查 设置
保持连接方式	
保持连接方式	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
保持连接方式	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
保持连接方式 会话保持 会话保持时间	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 ✓ 启用会话保持 1 小时 ▼ ①
保持连接方式 会话保持 会话保持时间 X-Fonwarded-For	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 ✓ 启用会话保持 1 小时 ▼ ① 在主属追加上—386010Hbbit
保持连接方式 会话保持 会话保持时间 X-Forwarded-For	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 ✓ 倉用会话保持 1 小时 ▼ ① 在末尾追加上一跳的IP地址 ▼
保持连接方式 会话保持 会话保持时间 X-Forwarded-For 头部政写	 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 □ □ □ ① 在末尾追加上一跳的IP地址 ▼ 新増 副除

头部改写	新增制的					
	四 类型	动作	参数名		参数值	操作
			暂无数据	n La		
防护方式						
BOT防护策略	暂不使用BOT防护策	略			•	
WEB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	1024	КВ			
响应检测	☑ 启用响应检测					
	响应检测body大小	1024	КВ			
真实客户端IP (i)	新增制					
真实客户端IP()	新増 割約			IP层数		操作
真实客户端IP ()	新増		暂无数据	IP层数		操作

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。

记录类型:	A- 将域名指向一个IPV4地址	\vee	
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【默试	从】线路… ∨	0
* 记录值:	5.5.5.5		

4.1.4.4. 效果预览

$\mathfrak{c} \leftarrow ightarrow \mathbf{C}$ 🛕 不安全 a.sangfor.com		as to to 🖞 🕲
🔎 Live Chat 🔍 +88 01 23 564		Login Register Help
AndHost	Home 🗸 🛛 Domain 🗸 Hosting 🗸 Services 🗸 P	^p ages ← Blog ← Contact
	Powerful Web Hosting Platform!	
	Start Today	
	ston	

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。

俄国部芬: 400-630-6430 SSL VPN 統一业务 安全接入平台	深信题科技手机官网 全面了解产品信息 上网行为管理 dows集成身份验证方法			
C 2004-2020 深信服料技版权所有			N.	

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。

🧑 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 <	BOT防护策略
@ 站点防护	新增 4 200余 凤用 颜用
ि 策略管理 2 ∨	□ 序号 BOT策略组 策略个数 描述
WEB防护策略	
BOT防护策略	
例外策略	
Co 安全防护规则库 >	
♀ SSL策略	
■ 黑白名単 >	
☞ 云端黑客IP防护	

组描述 请接 T子第略列表	1输入描述(远填)					
T子管略列表						
1 3 MICHAY SHA						
He Hile	启用 禁用					
序号	防护页面	请求接口	描述	启用/禁用	动作	操作

步骤2. 在设备[安全防护/站点防护]中创建站点防护。

🕢 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	站点防护 🌑 🛈			
G 站点防护 2	新增 3 启用 禁用	删除		
品 策略管理 >	序号 健康状态	站点名称	防护域	2
6 安全防护规则库 >				
♀ SSL策略				
□ 黑白名单 >				
☞ 云端黑客IP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。 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 本 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。

		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。
		● 加权最少连接
		表示选择(连接数/权重)最小的节点。
06	负载调度算法	● 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。
		● 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 >>>++++++++++++++++++++++++++++++++++
09	保持连接方式	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。
		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。
		● 在末尾追加上一跳的 IP 地址
11	X Forwarded For	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

		锁"两种。
		● 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。
18 19	响应检测 真实客户端 IP	检测 http/https 的相应 body 大小,最大支持 10M。 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 令暴破防护,以防止误封锁代理 IP。

基础信息

*站点名称	门户网站
*防护域名	1093
	添加
*服务类型	• http O https
*监听端口 ()	80 ×
	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	请输入
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	http * 10 .97 : 80
	添加
	☑ 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 /\RJ - ①
*X-Forwarded-For	在末尾追加上一跳的IP地址

头部改写	新增制除				
	□ 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	BOT防护策略			•	
WEB防护策略	暂不使用WEB防护策	略		•	展开详情 ▼
请求检测	请求检测body大小	1024 K	B		
响应检测	✓ 启用响应检测				
	响应检测body大小	1024 K	В		
真实客户端IP ①	新増 新				
	头部字段	言数	操作		
			暂无数据		

步骤4. 配置完成后,点击<确定>即可完成配置。

新汉		启用 禁用	20150	4	2部健康状态 ×		全部WEB防护策略×	•	全部BOT防护器	略 ×	•	站点名称/域名/监听	RП			C
	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/慧用	操作			
	1	正常	门户网站	10.90.8.93	http	80		暂不使用防护策略	6	BOT防护策略			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。

记录类型:	A- 将域名指向一个IPV4地址	~	
主机记录:	1.2.3.4.5.6	.dns-example.com	0
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 ∨	0
*记录值:	5.5.5.5		
* TTL:	10分钟	~	

← → C ▲ 不安全 | 10., . II.93/dwwa/login.php

* * 🔳

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。

DV	WA
Username	
Password	
0	Login

Damn Wilnerable Web Application (DVWA)

使用自动化工具(如Burpsuit)访问配置的BOT防护页面,访问失败

	cancel	host	10.90.8.93							
<	>	port	80	use SSL						
request										
raw paran	ms headers	hex								
Connection: Pragma: no- Cache-Contr Upgrade-Ins User-Agent: Safari/537. Accept: text/html, a change:v=b3 Refere: ht Accept-Lang Cookie: sec Cookie: sec	keep-alive cache colt no-cache secure-Reques Mozilla/5.0 36 pplication/x :==0.9 tp://10.90.8 ding: gzip, uage: zh-CN, surity=imposs 10afe3d624cb	ts: 1 (Windows N html+xml, ap .93/dvwa/lo deflate zh;q=0.9 ible: F14B3 06661af7880	[6.1; Win64; x; plication/xml;q; gin.php CEF1=001102fad9 [ac23965067e84e]	54) AppleW =0.9,image, 0570000000 1a2841abe9	ebKit/537.3 /avif,image, 003a00000000	6 (KHTML, /webp,imag 0648eb3560 d63ec;	like Gecko e/apng,*/* 00000014ec1) Chrome/99 ;q=0.8, app; p86003b1c2d	5.0.4638.17 lication/si; dd7:	gned-ex
F14B3CEF5=e	10afe3d624cb	06661af7880	ac239650e7e84e	1a2841abe9	a1391a901f5	d63ec;	0000001100			
Koule_WAF_J	007E64=D38dde	DUEDDaabdi J	110405166600a241							
+ < >										0 mot
+ < >										0 mat
+ < > response										_ 0 mai
+ < > response raw head	lers hex h	tml render	1							_ 0 mat
response raw head HTTP/1.1 20 Date: Sun, Content-Typ Content-Im Connection: Set-Cookie:	lers hex h 12 Accepted 18 Jun 2023 18 Jun 2023 18 Jun 2023 18 Jun 2023 18 Jun 2023 18 Jun 2023 18 Jun 2023 19 Jun	tml render 07:38:14 GM 01104041144	T 100000000320000	00000648eb4	46600000011	2ad15b33e6	4e34fe; pa	th=/: Max-/	4ge=86400	0 ma
+ < > response raw head HTTP/1.1 20 Date: Sun, Content-Iyp Content-Len Content-Iyn Content-Conkie: (1DOCTYPE h (html) (head)	lers hex h 12 Accepted 18 Jun 2023 18 Jun 2023 18 text/html gth: 284 keep-alive F14B3CEF1=0 xtml>	tml render 07:38:14 GM 01104041144	 r 1000000003a0000	00000648eb4	4660000001	2ad15b33e6	4e34fe; pa	th=/: Max-4	4ge=86400	_ 0 ma
+ < > response raw head HTTP/1.1 20 Date: Sun, Content-Ism Content-Ism Content-Ism Set-Cookie: (1D0CTYPE h (html) (head) (meta name= (a href="/d	lers hex h 12 Accepted 18 Jun 2023 18 Jun 2023 18 text/html gth: 284 keep-alive F14B3CEF1=0 xtml> "r" content= 12 cmyrs1JsXJx	tml render 07:38:14 GM 01104041144 "11NNyWiqmC ZwlJjY"> <th>] t a000000003a0000</th> <td>00000648eb+</td> <th>1660000001</th> <th>2ad15b33e6</th> <td>4e34fe; pa</td> <th>th=/: Max-1</th> <td>Age=86400</td> <td> 0 ma</td>] t a000000003a0000	00000648eb+	1660000001	2ad15b33e6	4e34fe; pa	th=/: Max-1	Age=86400	0 ma
+ < > response raw head HTTP/1.1 20 Date: Sun, Content-Iyp Content-Len Content-Iyp Content-Iyp Content-Iyp Content-Iyp Content-Iyp (head) (head) (head) (head)	lers hex h 12 Accepted 13 Jun 2023 18 Jun	tml render 07:38:14 GM 01104041144 "11NNyWiqmC ZwlJjW">script" cha script" cha script ches not	1 a000000003a0000 (X2raG1MG"> > > set="utf-8" sr support Java3	00000648eb 2="/T1NNyW Script! 1</td <th>1660000001: iqmCIX2raGl) ioscript></th> <th>2ad15b33e6 MG″≻<td>4e34fe; pa pt></td><th>th=/; Max-1</th><td>4ge=86400</td><td> 0 m:</td></th>	1660000001: iqmCIX2raGl) ioscript>	2ad15b33e6 MG″≻ <td>4e34fe; pa pt></td> <th>th=/; Max-1</th> <td>4ge=86400</td> <td> 0 m:</td>	4e34fe; pa pt>	th=/; Max-1	4ge=86400	0 m:

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

(90 <	cancel >	host 1 port 8	0.90.8.93	use 🗌	SSL					
reques	t		2								
raw	params	headers hex									
GET /d	lvwa/login	.php HTTP/1.1									-
Host: Connec	10.90.8.9 tion: kee	o-alive									
Pragma	: no-cach	ie									
Cache-	Control: le-Insecur	no-cache									
User-A	lgent: pyt	hon									
Accept	:										
text/r	tmi, appii ∵v=b3∵o=0	.cation/xhtml+x 1.9	mi, applic	ation/xπ	u:q=0.9,	1mage/a	vit, image/webp,	image/:	apng, */	*:q=0.8, application/signed-	ex
Refere	r: http:/	/10.90.8.93/dv	wa/login.	php							
Accept	-Encoding	: gzip, deflat	e								
Cookie	: securit	y=impossible;	F14B3CEF1	=001102f	ad905700	0000000	3a00000000648et	356000	000014e	cb86003b1c2dd7;	
F14B30	EF5=e10af	e3d624cb06661a	f78801ac2	39650e7e	84e1a284	1abe9a1	391a901f5d63ec;				
Koule_	WAF_307E6	4=b38ddebUebba	abdf 34f 04	.U5166bUa	241						
											-
+	< >									0	matches
respon	50 0										
row	boodors	Khox Khtml Kr	rondor								
UTTD/1	1 402 E-	whidden	Telluel								
Date:	Sun, 18 J	un 2023 07:40:	14 GMT								Ê
Conter	t-Type: t	ext/html									
Conter	t-Length:	171787 n-alive									
ETag:	"629ee387	-29f0b"									
<pre></pre>	YPE html>	``````````````````````````````````````									
<head></head>	Tang- on	-									
<	meta char:	set="UTF-8">									
< /	title>版版 etvle>	か 狂鹿									
	body {										
	h	eight: 100vh	:								
	w	idth: 1009w; argin: 0									
	p	adding: 0;									
	1 b	ackground-co	lor: #f7	f9fc:							
	1										-
BOT防护日	志					常规					
时间范围	2023-06-18 0	00:00-2023-06-18 23:59		严重等级	🖾 高位 🖸	etill :	2023-06-18 15:40:14	协议:	нттр	回复状态码: -	
攻击类型	所有类型		*	XFF IP (j)	全部	攻击典型: 产量等级:	思想USER-AGENT	方法:	GET	DEBCEWARE: 1 THOMSE	
泉田日志						URL :	10.90.8.93/dvwa/login.php				
78	対側	攻击侯型	(#IP	源中日尾坎	URL	检测节点:	waf-127.0.0.1				
1	2023-06-18 15:40:1	4 恶意USER-AGENT	200.200.148.55	ea	10.90.	User-Agent 描述:	: python 检测到此用户请求命中USER-AGE	ENT黑名单,信用	非法客户通进行	i81 9 .	
2	2023-06-18 14:25:1	7 恶意USER-AGENT	200.200.148.55	巴西	asanc	危害说明:	客户講可以還过自助化程序恶意功	(击设备服务器,)	以达到篇阅探测	则用、暴力破解、拒绝服务攻击、蹲羊毛、数据施取尊非法目的。	
3	2023-06-18 14:21:5	8	200.200.148.55	PE	a.sanc	参考信息:					
4	2023-06-18 14:20:1	6 恶意USER-AGENT	200.200.148.55	EE	a.sanc	深值服Wiki					
5	2023-06-18 11:37:1	1 BOT工具描纹	200.200.148.55	25	a.sanc	-					
6	2023-06-18 11:33:0	2 恶意USER-AGENT		PB	a.sanc	28 (BIP :	200.200.148.55	遵納口:	53458		
7		1 BOT工具指纹		es	a.sanc	源IP归属地:	巴西	XFF IP :	12.		
8	2023-06-18 11:32:1	0 BOTT員指纹		PE	a.sanc	数据包					TU TT 01
0	2023-06-18 11:31-3	2 前赤金建	200.200.148.55	ea		RECHIEST.					
10		0 3100 020	200.200.148.55	pres		GET /dvwa/	login.php HTTP/1.1				
	2022-06-19 11-20-5	2 Ege (CCD-ACTA)	200.200.140.55	px	esalt	Host: 10.90 Connection	8.93 : keep-alive				
	2022 05 10 11:29:3		200.200.140.35		esant	Pragma: no	-cache				
	2023-00-18 11:23:4	a and to ser-agent	200.200.148.55	CA	asanç	Cache-Cont Upgrade-In	roi: no-cache secure-Requests: 1				
	2023-00-18 11:23:4	2 · 思想USER-AGENT	200.200.148.55	CA	a.sanç	User-Agent Accept: text	: python :/html.application/vhtml+vml +or	lication/wmhra=	0.9 image/aulti	mage/webp.image/apng.*/*:g=0.8 application/signed-avchappe	ev=b3:g=0.
						9			,	2. Formal should be available and all and available	
						Referer: htt	p://10.90.8.93/dvwa/login.php				
						添加伊约	N			当台京县,1 上一条	N-44

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。

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	WEB防护策略			
G 站点防护	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		建议在日常运维业务保护场景下使用,选取最准确的规	则对命中的攻击进行拦截,其余规则命中后仅;
WEB防护策略 3	- 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	,提供漏洞防扫描能力,针对恶意的漏洞扫描
BOT防护策略				
例外策略				
6 安全防护规则库				
♀ SSL策略				
3 黑白名单	>			
G 云端黒客IP防护				
*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 ①			
云端威胁情报	✔ 云端黑客IP防护 ①			
协议保护			₩ ★ 数防护	
in oction		温度的 二 (
	CONTROL	MILLICHICHICAL		
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。

众 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	站点防护 🔵 ①
G 站点防护 2	新增 3 四用 禁用 翻除
品 策略管理 2000 201	□ 序号 健康状态 站点名称 防护域名
G 安全防护规则库 >	
② SSL策略	
□ 黑白名单 >	
G 云端黑客IP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。 ● 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 令暴破防护,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。

站点名称	站点防护		
防护域名	10.243.3.67		
	添加		
监听端口 ①	80 ×		
	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	请输入		
防护方式		-	
BOI防护策略	習不使用BOI 防护策略	Ť	
WEB防护策略	WEB防护策略	*	展开详情
检测动作	 	ż	
检测动作 联动封锁	 检测后放行 检测后拦着 启用联动封锁 ① 		
检测动作 联动封锁 真实客户端IP ①	 	ē.	
检测动作 联动封锁 真实客户端IP ①	 	t IP层数	操作
检测动作 联动封锁 真实客户端IP ①	 检测后放行 ● 检测后拦截 自用联动封锁 ① 新增 删除 头部字段 	1 IP层数 暂无数据	操作

步骤4. 配置完成后,点击<确定>即可完成配置。

8F)		AR MR BIA			金部WEB助护策略 × •	全部BOT防护策略 ×	•	5/旅行第日 Q	C
	序号	站点名称	防护城名	监听第口	WEB肋护策略	BOT防护策略	启用/禁用	操作	
	1	站后防护	10.243.3.67	80	WEB防护策略	暂不使用BOT策略		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;
nid /var/run/nginx.pid:
load_module /etc/nginx/ngx_1.21.6_http_waf_agent_module.so;
events {
    worker_connections 1024;
http {
    include /etc/nginx/mime.types;
default_type application/octet-stream;
     include
    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。



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:

#custor	n 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。

403 Forbidden	
top forbidacti	

nginx/1.21.6

	监控 安全防护	中 节点管理	日志管理	系统管理	详情						
-				_	基础信息						
安全日応				_	常规						
时间范围	2022-04-20 17:00-2022	2-04-20 23:59	严重等级	🗹 致命 🛛 🔽 英信	时间:	2022-04-20 17:28:31	协议:	HTTP	黄型:	SQL注入	
协议类型	http 🔽 https			☑ 允许 ☑ 拒绝	方法:	GET	回复状态码	6	严重等级:	 中危 	
					动作:	拒绝	匹配站点名	: 站点防护			
					URL:	10.243.3.67/?id=1;select user	mame from userin	nfo where userid=1			
19.22	811121	R±HR	at 21,267	-7610	描述:	攻击语句: ;select username f	rom u				
12-5	23(6)	0.0962	1000794C14	2201	危害说明:	攻击者利用此漏洞盗取数据库中	·数据、导致WEB业	务信息泄漏,危及数据库账。	自信息安全 。		
	2022-04-20 17:28:31	Web应用防护	SQL注入	10.243.3.56	规则ID:	13020047					
2	2022-04-20 17:28:31	Web应用助护	SQL注入	10.243.3.56	规则名称:	Select语句SQL注入攻击					
				_	检测节点:	waf-127.0.0.1					
					参考信息:	2					
					解决方案:	-					
					深信服Wiki:	https://sec.sangfor.com.cn/se	ecurity-vulnerabili	ty/detail?vuln_sfv=SF_000	0_00086⟨=ZH-CN		
					10						
					IIIP:	10.243.3.56	源法口:	60640			
					源)P(回屬地:	2	XFF IP:	121			
					数据包						TU TT 1
					INCLUDE EN	CODING TYPE: URL					
					REQUEST:						
					GET /?id=1;	select username from userinfo	where userid=1 H	ITTP/1.1			
					Host: 10.243	1.3.67					
					Lograde-log	Reep-alive					
					User-Agent:	Mozilla/5.0 (Windows NT 6.1:)	Win64; x64) Apple	WebKit/537.36 (KHTML li	ke Gecko) Chrome/100.0	1.4896.127 Safari/537.36	Edg/100.0.118
					5.44						
					Accept: text,	/html,application/xhtml xml,ap	plication/xml;q=0	1.9, image/webp, image/apr	ig,*/*;q=0.8,application/f	igned-exchange;v=b3;c	=0.9
					Accept Spec	dings only 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。



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。
- 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<u>2.3章节</u>和 <u>3.3章节</u>。

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。

根据提示输入密码(与安装密码一致)。

[root@waf-fefcfe0dd06a h	ome]# monitor uninstall ent Platform + WAE Agent
beptoyment Rote: Hanagem	ene Flactoria i anti Agente
Selected Module: Uninsta	ll All
Password to Uninstall: *	****************
[+] Running 4/4	
<pre># Container waf_redis</pre>	Stopped
<pre># Container waf_detect</pre>	Stopped
<pre># Container waf_mgt</pre>	Stopped
<pre># Container waf_nginx</pre>	Stopped
Going to remove waf_ngin	x, waf_detect, waf_redis, waf_mgt
[+] Running 4/4	
<pre># Container waf_mgt</pre>	Removed
<pre># Container waf_nginx</pre>	Removed
<pre># Container waf_detect</pre>	Removed
<pre># Container waf_redis</pre>	Removed
Untagged: waf_nginx:8.0.	60.308B
Deleted: sha256:b6b10141	34acd121d736a6ad7b2bc358140dfdaa3fd5210827690275fdb70f97
Deleted: sha256:c5b6fdaf	7792f066efaa72f3c5d46cb31d76cde1580d9b5f42f9e1d39c50b451
Deleted: sha256:181a37e0	176d63762df9f4ba52bc003a258c996d12ee36d545b2525e6086ac1e
Deleted: sha256:cb9826d9	12cc07dc6b870001d6fb84ca9adcb7007af94269f9e6e3206f146fe5
Deleted: sha256:89ffc978	fa6f33a518fec15dcb9282689b75804d0761a48cb957362e901db4f2
Deleted: sha256:6882c6a9	dad9ab09b1e5d5e058324a471e437a00a2c07dd6bc67981221fb571b
Untagged: waf_detect:8.0	.60.308B
Deleted: sha256:cd256ae8	25617841d41d10bf19ab6139746bb83ac13809229933679a43130b63
Deleted: sha256:151f372b	96e628afeb2fe9f252b799c6f43719d6b8d97242df457b87500fb556
Deleted: sha256:34c3216c	4048cc8684d2fa2595ab417111d0dd102c2b52c56c903ea21a2d5bcf
Deleted: sha256:647e93dd	000755c2d1c2dd97e12fbd2363d3146af23dd5da92c59da47e0279e4
Deleted: sha256:d09592b3	ba6c6ea467a1599e54acfee8da35815c17fc8340a43795fd5064912c

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。