



天融信云防火墙系统 部署实施指导书（华为云）



北京市海淀区西北旺东路 10 号院西区 11 号楼 1 层 101 天融信科技集团 100193

电话: 010-82776666

传真: 010-82776677

服务热线: 4007770777

<http://www.topsec.com.cn>

版权声明

本文档中的所有内容及格式的版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有 不得翻印 © 2025 天融信公司

商标声明

本文档中所谈及的产品名称仅做识别之用。文档中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC® 天融信公司

信息反馈

<http://www.topsec.com.cn>

[illegible]

注：对该文件内容增加、删除或修改均需填写此记录，详细记载变更信息，以保证其可追溯性

目录

1.	产品简介	1
2.	部署环境要求.....	1
2.1.	版本特性	1
2.2.	镜像获取	1
2.3.	产品规格	1
2.4.	授权方式	4
2.5.	注意事项	4
3.	部署实施	4
3.1.	华为云	4
3.1.1.	登华为云	4
3.1.2.	上传镜像至存储桶.....	5
3.1.2.1.	创建存储桶	5
3.1.2.2.	上传镜像.....	7
3.1.2.3.	获取镜像 URL	8
3.1.3.	创建自定义镜像.....	9
3.1.4.	部署安全网元.....	12
3.1.4.1.	购买云服务器	12
3.1.4.2.	确认部署成功	16
3.1.5.	配置网络和安全组	17
3.1.6.	设备登录	18
4.	设备授权	19
4.1.	云安全管理平台授权.....	19
4.1.1.	平台部署	20
4.1.2.	授权申请	20
4.1.3.	授权导入	20
4.1.4.	下发授权	21
4.2.	LICENSE-CONTROLLER 授权.....	23
5.	基础配置指导.....	23
5.1.	WEB 应用防火墙	23
5.1.1.	模式部署	23
5.1.1.1.	代理模式.....	23
5.1.1.2.	部署拓扑.....	24
5.1.1.3.	基础配置.....	24
6.	常见问题	26
6.1.	无法自动获取 IP 问题	27
6.2.	授权是提示“无可用授权”	27
7.	注意事项	27

1. 产品简介

目前大量用户为降低运维复杂度并满足数据本地化需求，采用公有云托管业务。然而，公有云架构在安全防护能力上存在不足，需依赖第三方安全虚拟化组件弥补短板。针对这一需求，天融信推出了适配公有云环境的云防火墙解决方案，支持信创（ARM/海光）及非信创（x86）架构。该方案支持通过云平台镜像模板快速部署，并针对离线环境（如无法连接公网或授权服务器）提供本地化授权服务器方案，实现批量授权管理。此外，云防火墙版本针对公有云环境特性进行了专项优化，适配云上场景及需求。

2. 部署环境要求

2.1. 版本特性

2.2. 镜像获取

2.3. 产品规格

版本	功能差异	推荐系统盘大小	推荐 CPU 核数	推荐内存	推荐数据盘大小	最优网卡队列数
标准版	20Mbps、2W 并发、2 服务器策略性能授权及 WAF 规则库、地理信息库许可。	100G	2	8G	数据盘：无（可无需数据盘）	1
专业版	50Mbps、3W 并发、5 服务器策略性能授权及 WAF 规则库、地理信息库许可。	100G	2	8G	数据盘：无（可无需数据盘）	1
高级版	100Mbps、6W 并发、10 服务器策略性能授权及 WAF 规则库、地理信	100G	2	8G	数据盘：无（可无需数据盘）	1

	息库许可。					
增强版	200Mbps、12W并发、20 服务器策略性能授权及 WAF 规则库、地理信息库许可，并且包含网页防篡改、漏洞扫描引擎。	100G	4	16G	数据盘： 200G（推荐最低值）	3
旗舰版	500Mbps、12W并发、20 服务器策略性能授权及 WAF 规则库、地理信息库许可，并且包含网页防篡改、漏洞扫描引擎。	100G	4	16G	数据盘： 200G（推荐最低值）	3
旗舰版-1000	1000Mbps、12W 并发、30 服务器策略性	100G	8	16G	数据盘： 200G（推荐最低值）	7

	能授权及 WAF 规则库、地理信息库许可，并且包含网页防篡改、漏洞扫描引擎。					
旗舰版-2000	2000Mbps、15W 并发、40 服务器策略性能授权及 WAF 规则库、地理信息库许可，并且包含网页防篡改、漏洞扫描引擎。	100G	16	16G	数据盘： 200G（推荐最低值）	15
旗舰版-4000	4000Mbps、20W 并发、50 服务器策略性能授权及 WAF 规则库、地理信息库许可。	100G	32	32G	数据盘： 200G（推荐最低值）	31

可，并且包含网页防篡改、漏洞扫描引擎，同时支持混合模式（流模式+代理模式同时）。					
--	--	--	--	--	--

2.4. 授权方式

参考第四章节，设备授权。

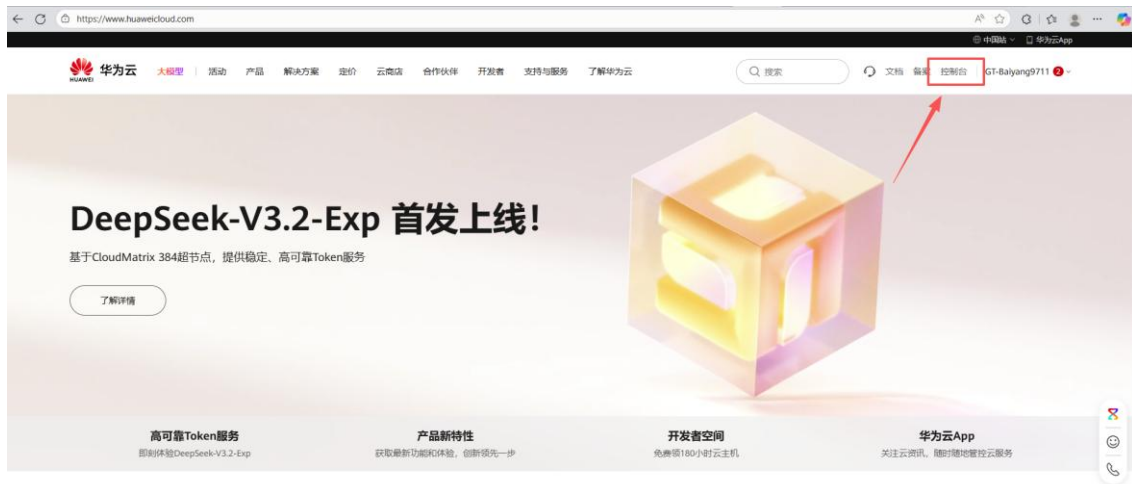
2.5. 注意事项

3. 部署实施

3.1. 华为云

3.1.1. 登华为云

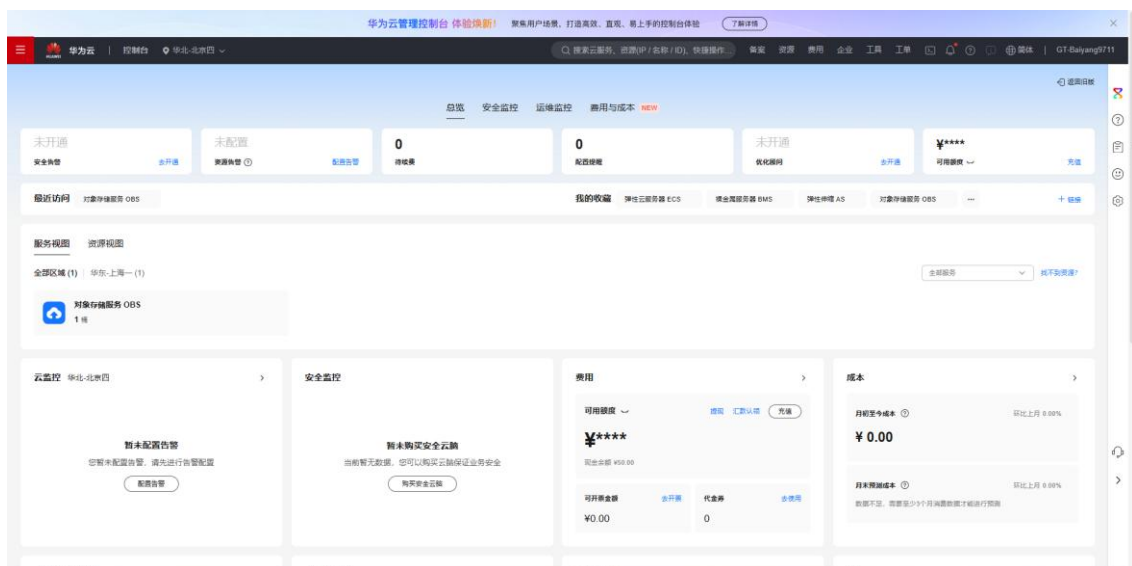
第一步：登陆华为云中国站[行业 AI 先锋-华为云](#)，点击右上角控制台，点击进入。



云上AI，敏捷创新重塑千行百业

<https://www.huaweicloud.com/ai/token-service.html>

第二步：进入到华为 ECS 管理控制台。

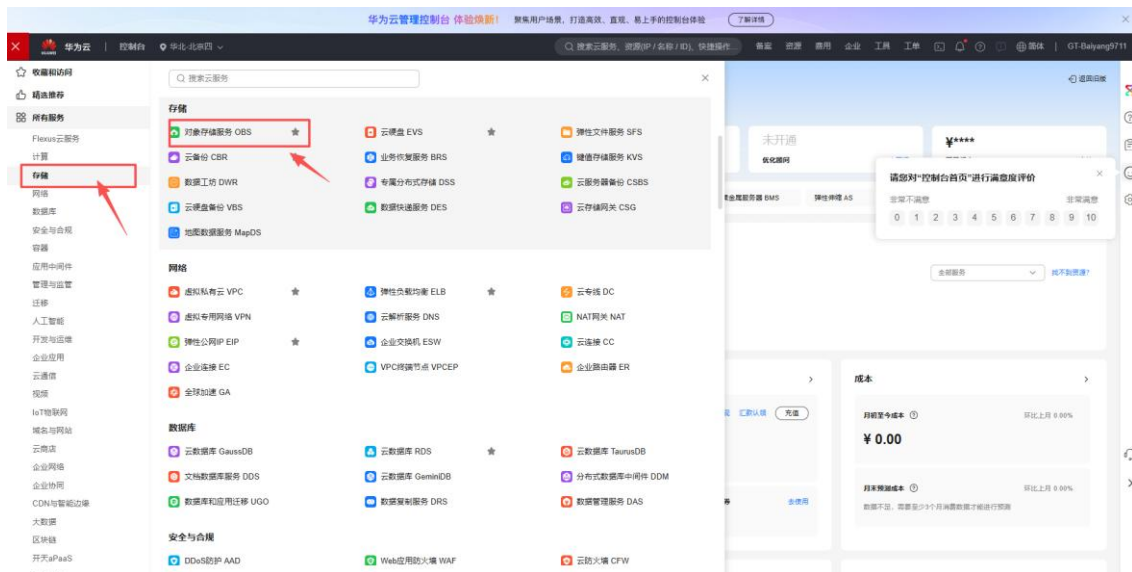


3.1.2. 上传镜像至存储桶

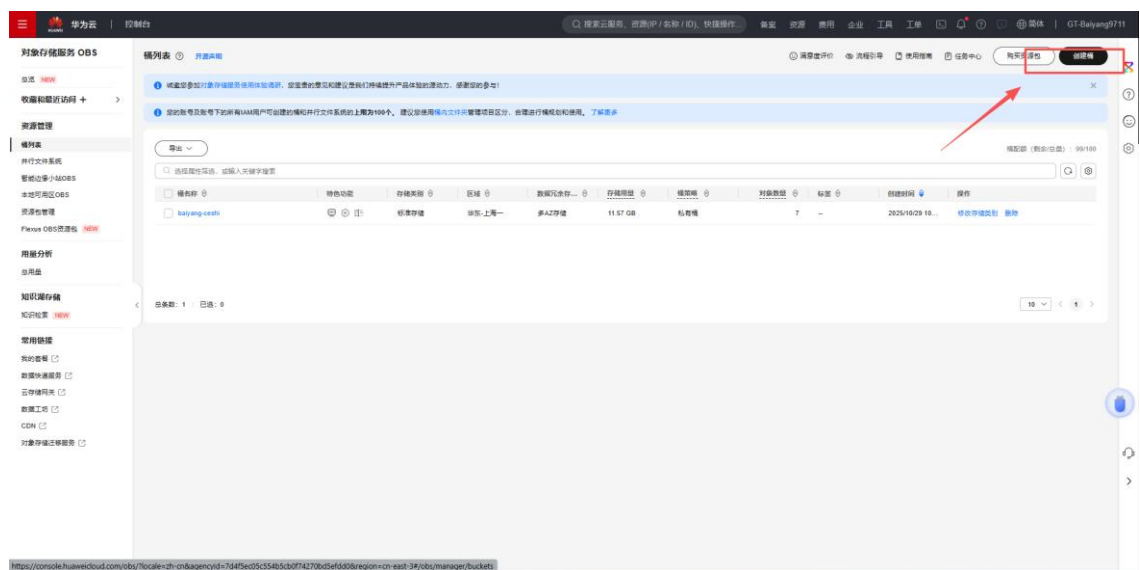
3.1.2.1. 创建存储桶

需要将自己的 qcow2 镜像，需要上传至华为云“对象存储服务 OBS”中的存储桶中，才可在华为云平台上创建相应的镜像文件

第一步：点击左上角菜单栏，点击【对象存储服务 OBS】，进入到对象存储。

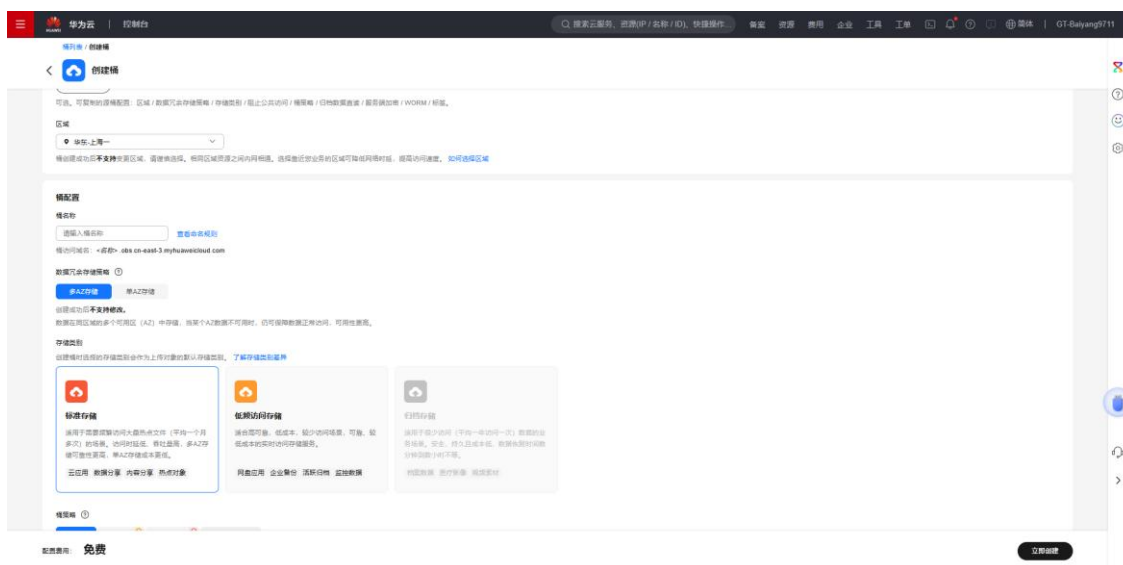


第二步：点击存【桶列表】，若客户环境已具备存储桶可直接使用，若不具备则需要点击【新建】，重新创建存储桶。



第三步：填写存储桶名称，选择地域，其余可按默认配置，然后点击“完成创建”。

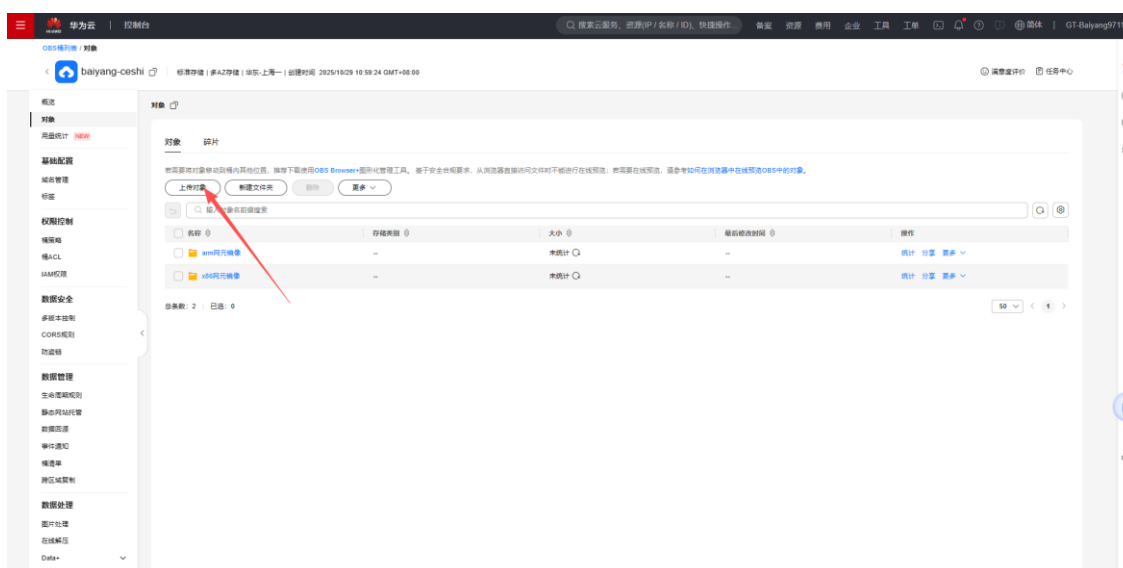
此处需注意：“区域”需要与“创建安全网元的 OBS 服务器地域”相同。



3.1.2.2.上传镜像

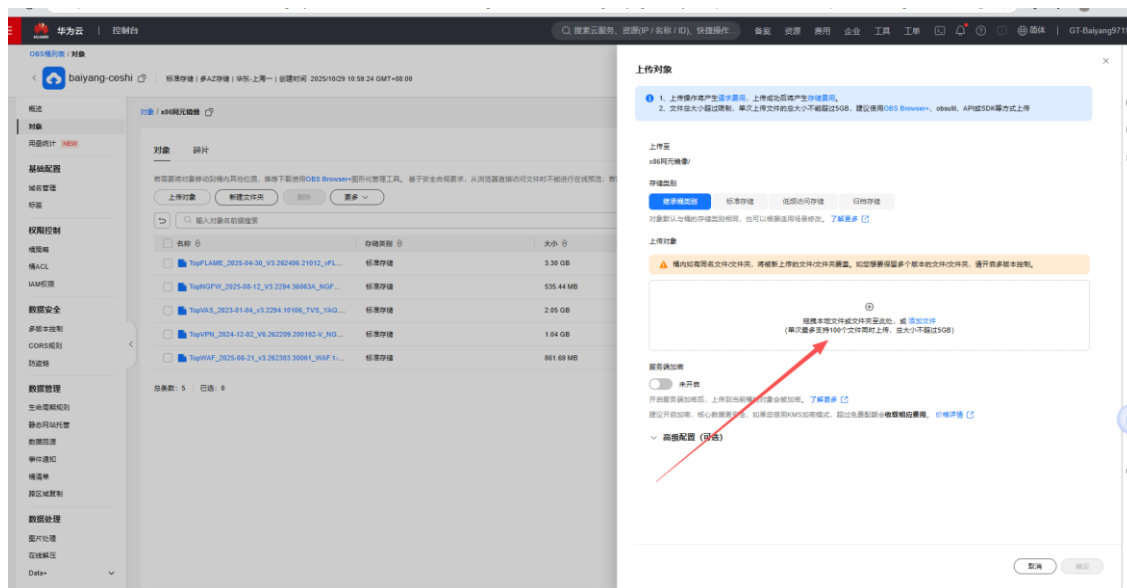
第一步：进入到创建好的存储桶中，点击上传文件。

提示：可以提前将桶的分类创建好，后续镜像文件无法移动；

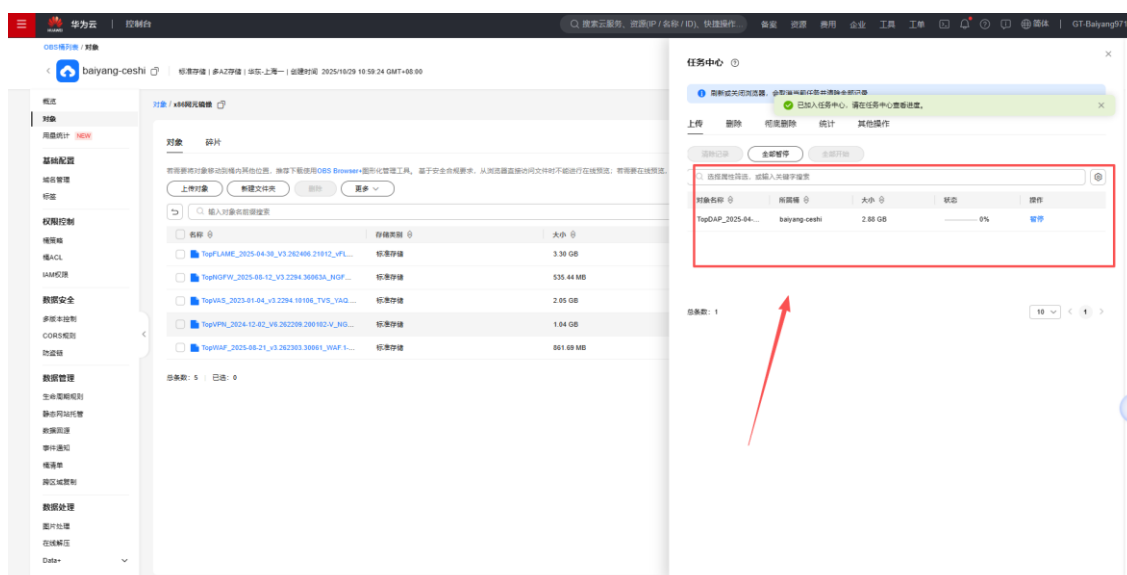


第二步：进入到上传文件页面后，有两种上传形式，

- 1、点击选择文件，选择终端上的文件进行上传；
- 2、直接将需要上传的文件拖转至上传区域。（**单次传输的总大小不能超过 5 个 G**）



第三步：点击【上传】等待上传完成。

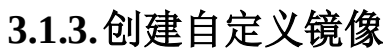


3.1.2.3. 获取镜像 URL

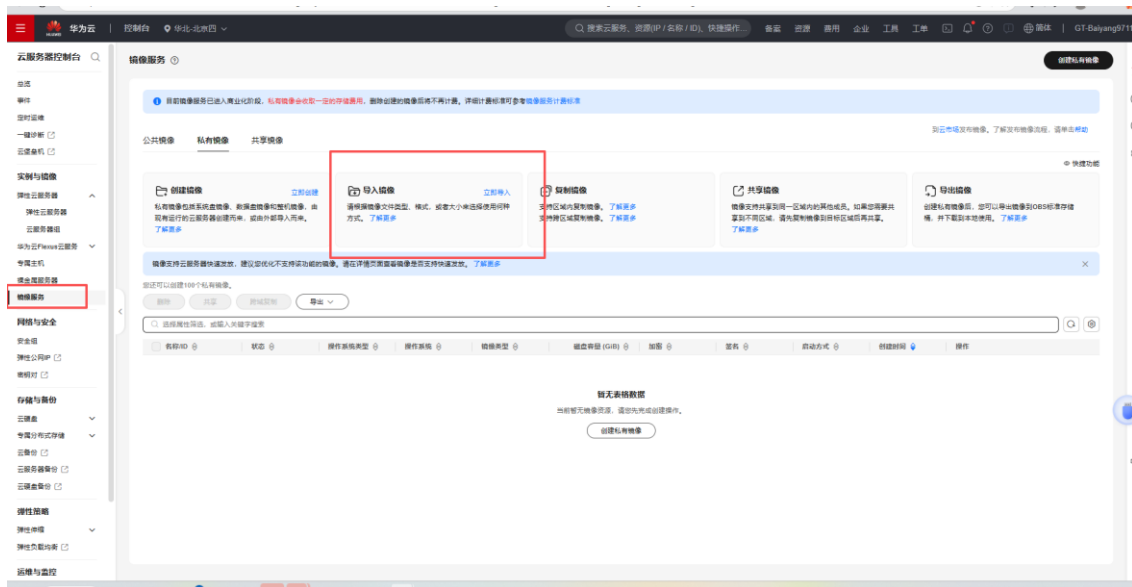
第一步：点击已上传至存储服务的文件“分享”

第二步：此处获取文件的 URL 地址，以及分享该文件的链接。

注意：该 URL 与其他用平台有所差异，点击 URL 是直接下载该镜像(华为云在创建自定义镜像时不用镜像 URL)



第二步： 点击“镜像服务”，进入镜像页面。然后点击“导入镜像”。



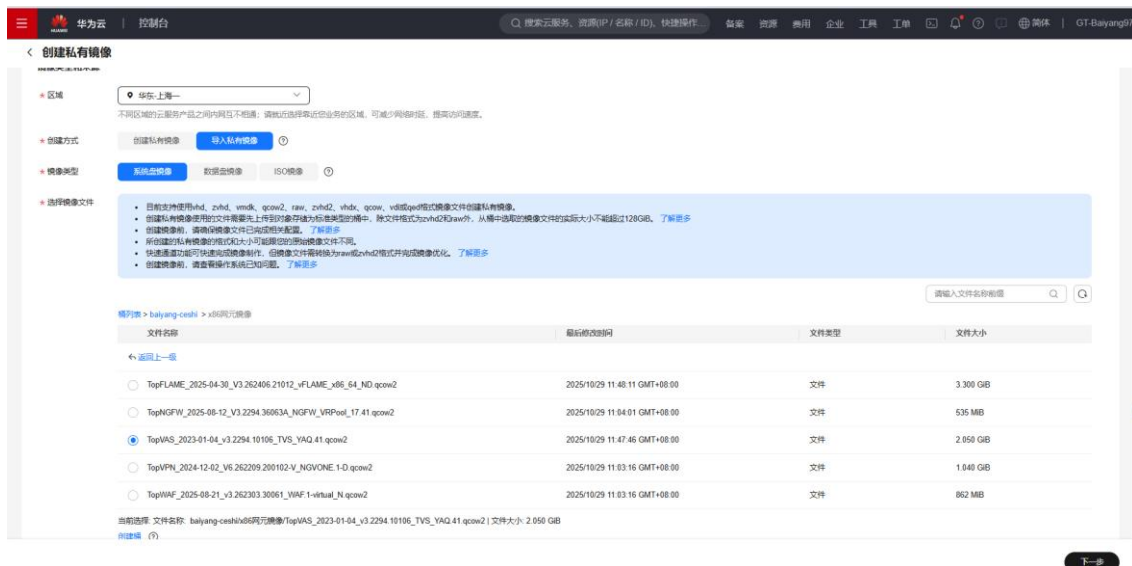
第三步：

【区域】选择为桶创建的区域。

【创建方式】选择导入私有镜像

【镜像类型】：选择系统盘镜像

【选择镜像文件】选择您想要常见的自定义镜像文件



配置信息：

镜像用途：ECS 系统盘镜像

架构类型：x86 或者 ARM（根据所要创建的自定义镜像架构选择）

启动方式：x86 的选择 BIOS，ARM 选择 UEFI

操作系统：x86 选择 Other/Other Linux（64bit），ARM 选择相同

系统盘：100G

创建私有镜像

启动方式: BIOS UEFI

操作系统: Other Other Linux(64 bit)

系统盘 (GB): 100

名称: 天融信漏洞

加密: ☐ KMS 加密

标签: 标签键 标签值

描述: 0/1,024

协议: ☒ 我已仔细阅读并同意《镜像制作承诺书》和《镜像免责声明》

下一步

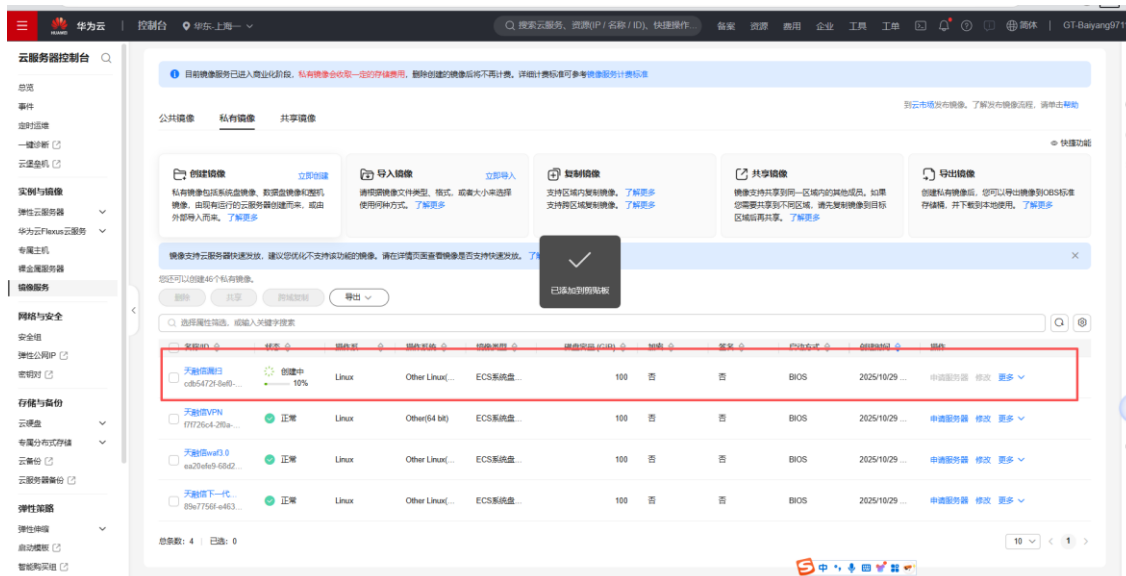
第四步：其余选项可按需选择，如不需要默认为不设置，点同意协议，点击“下一步”并点击“提交”。

资源详情

产品名称	配置	数量																
系统盘镜像	<table><tr><td>区域</td><td>华东-上海一</td></tr><tr><td>镜像类型</td><td>ECS系统盘镜像</td></tr><tr><td>名称</td><td>天融信漏洞</td></tr><tr><td>来源</td><td>镜像文件 (TopNAS_2023-01-04_v3.2294.10106_TV8_YAQ.41.qcow2)</td></tr><tr><td>操作系统</td><td>Other Linux(64 bit)</td></tr><tr><td>系统盘 (GB)</td><td>100</td></tr><tr><td>架构类型</td><td>x86</td></tr><tr><td>启动方式</td><td>BIOS</td></tr></table>	区域	华东-上海一	镜像类型	ECS系统盘镜像	名称	天融信漏洞	来源	镜像文件 (TopNAS_2023-01-04_v3.2294.10106_TV8_YAQ.41.qcow2)	操作系统	Other Linux(64 bit)	系统盘 (GB)	100	架构类型	x86	启动方式	BIOS	1
区域	华东-上海一																	
镜像类型	ECS系统盘镜像																	
名称	天融信漏洞																	
来源	镜像文件 (TopNAS_2023-01-04_v3.2294.10106_TV8_YAQ.41.qcow2)																	
操作系统	Other Linux(64 bit)																	
系统盘 (GB)	100																	
架构类型	x86																	
启动方式	BIOS																	

上一步 提交

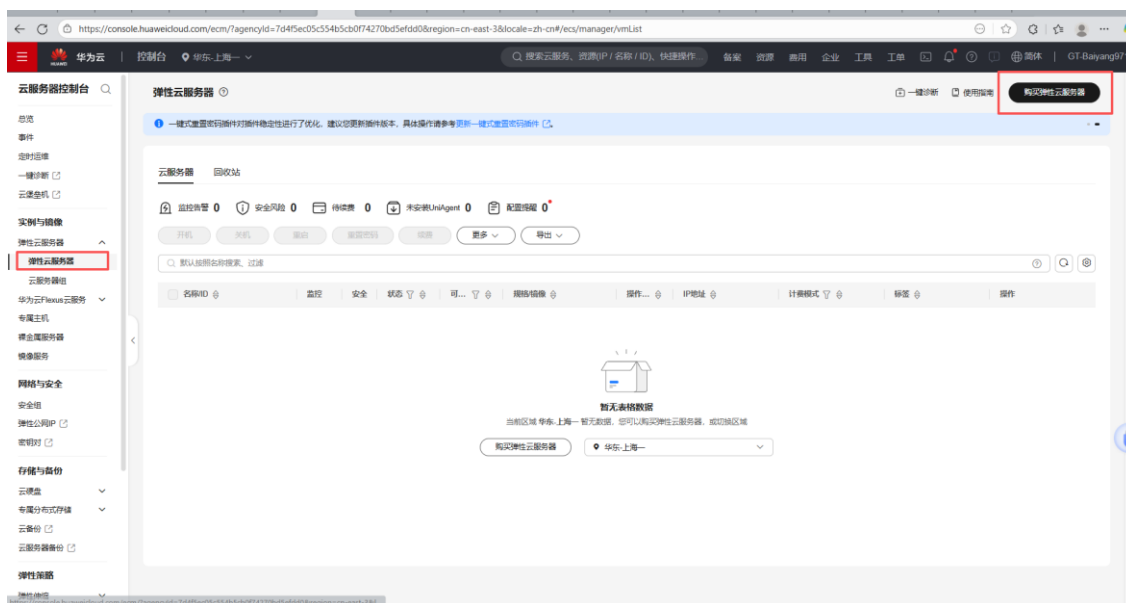
第四步：创建完成即为创建成功。

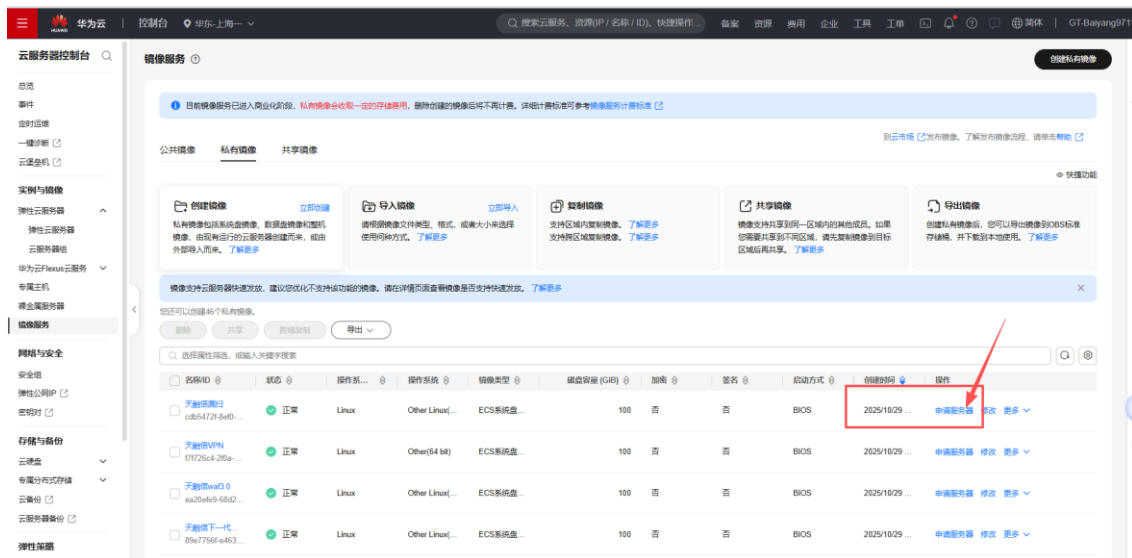


3.1.4. 部署安全网元

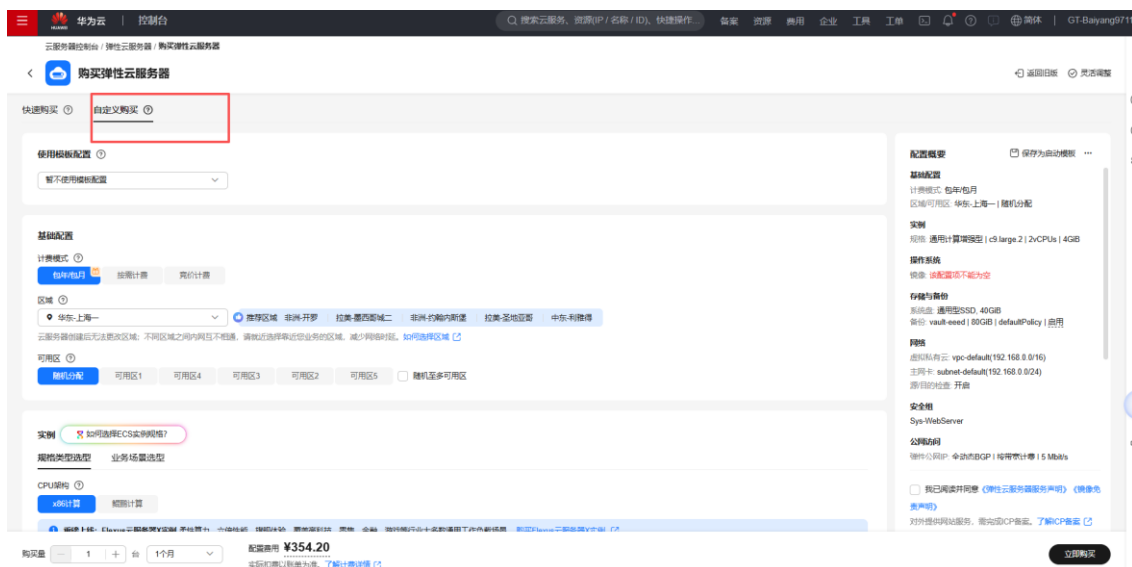
3.1.4.1. 购买云服务器

第一步：进入云服务器 ECS 控制台，点击“弹性云服务器”，点击右上角“购买弹性云服务器”。或直接在自定义镜像下，点击“创建服务器”也可跳转至购买页面。





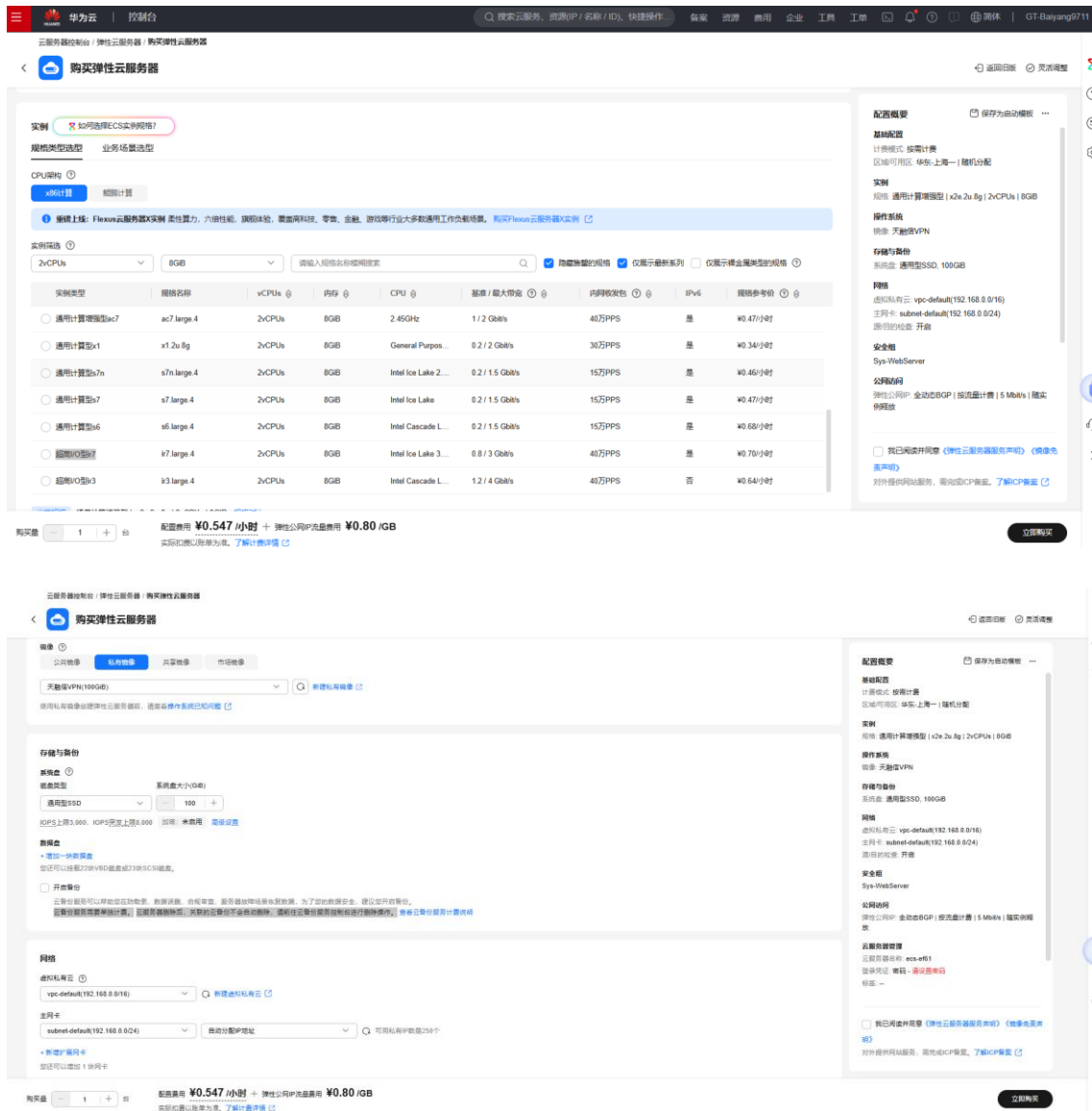
第二步：点击“自定义购买”。

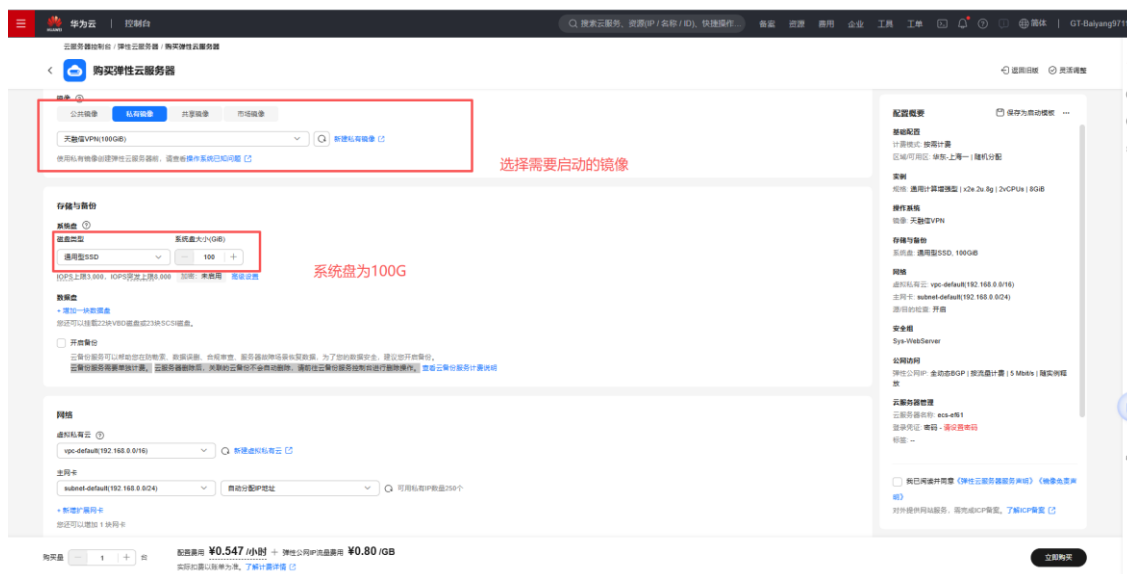


第三步：配置需要启动的镜像服务器配置

- 1、地域：按用户需求选择，此处需要与自定义镜像地域一致，并且与用户业务 ECS 相同地域。
- 2、网络与可用区：按用户需求选择，尽量与用户业务 ECS 相同。
- 3、机型：根据产品规格和云安全产品管理中心推荐机型选择。【重点】
- 4、镜像：选择自定义镜像中的需要启动的镜像；
- 5、系统盘：100G
- 6、数据盘：根据需求添加

- 7、备份功能：华为云具有数据备份功能，云备份服务需要单独计费。云服务器删除后，关联的云备份不会自动删除，请前往云备份服务控制台进行删除操作。

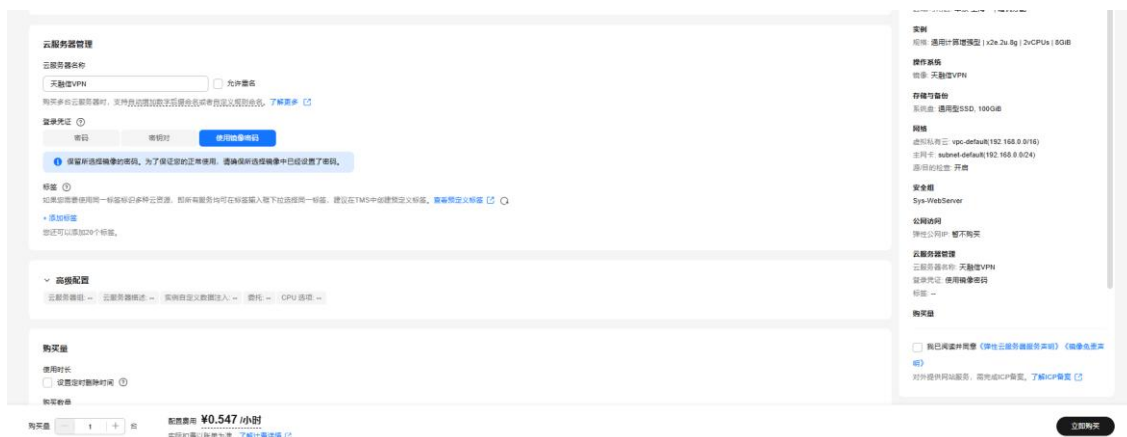




第四步：配置网络部分。

- 1、公网 IP：此处可按需选择。
- 2、安全组：此处按默认即可，后续 3.1.5 章节进行详细配置。
- 3、网卡：网卡按需选择，默认一张网卡即可。
- 4、登录凭证：使用镜像密码



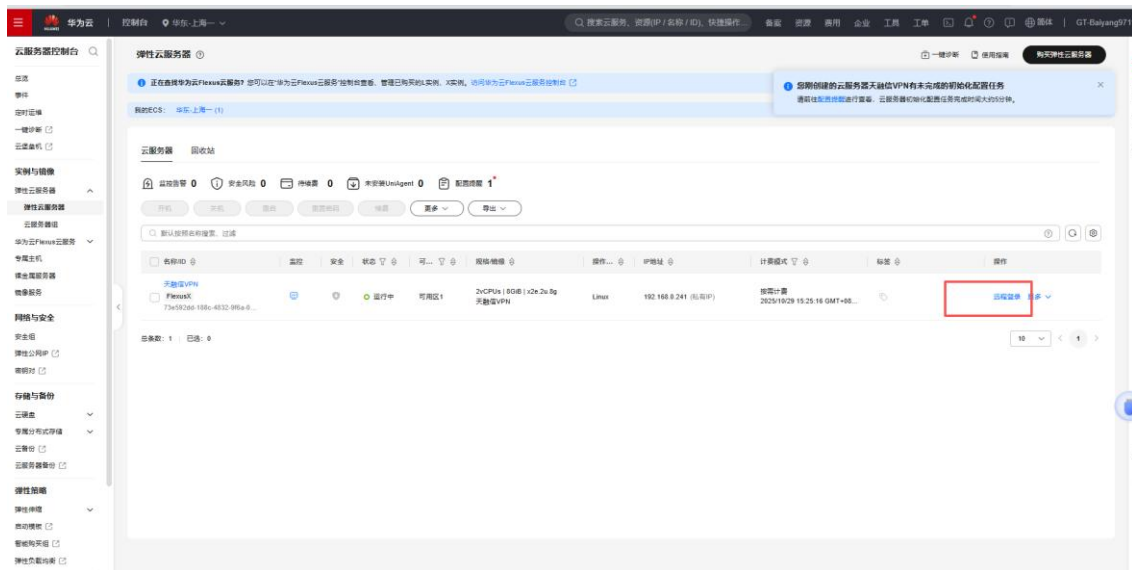


第五步：购买成功

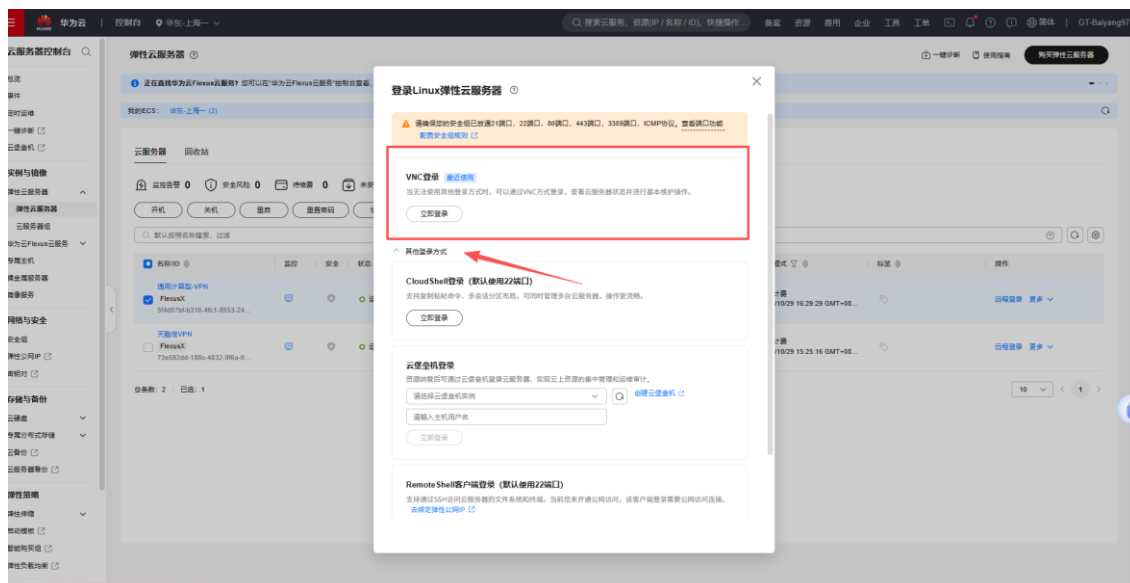
点击同意授权，点击立即购买，购买成功。

3.1.4.2. 确认部署成功

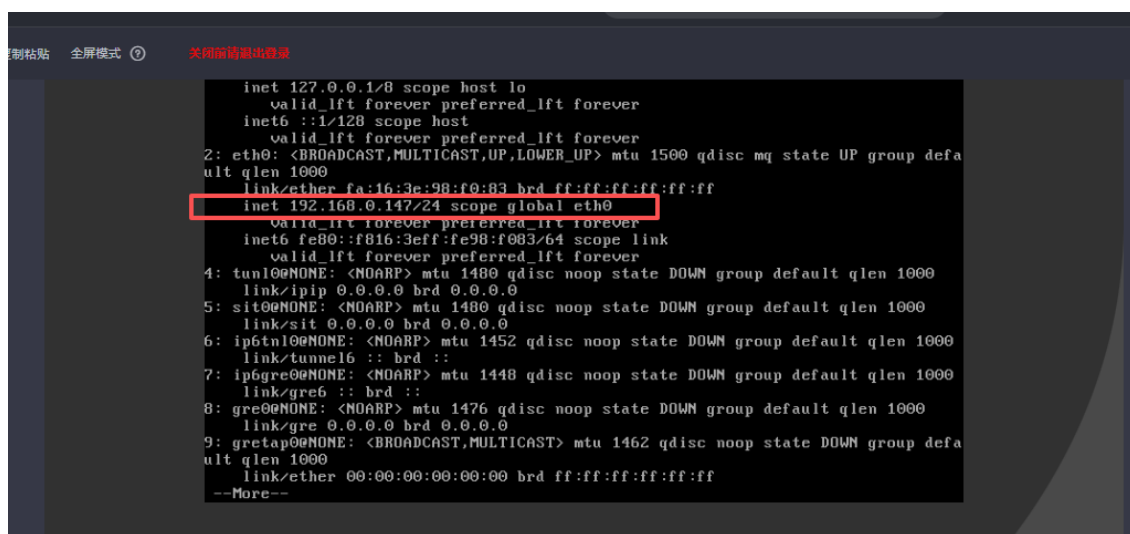
第一步：进入到云服务器控制台，点击“远程登录”



第二步：选择通过 VNC 远程连接，首次连接时 VNC 登录在“其他登录方式”里。

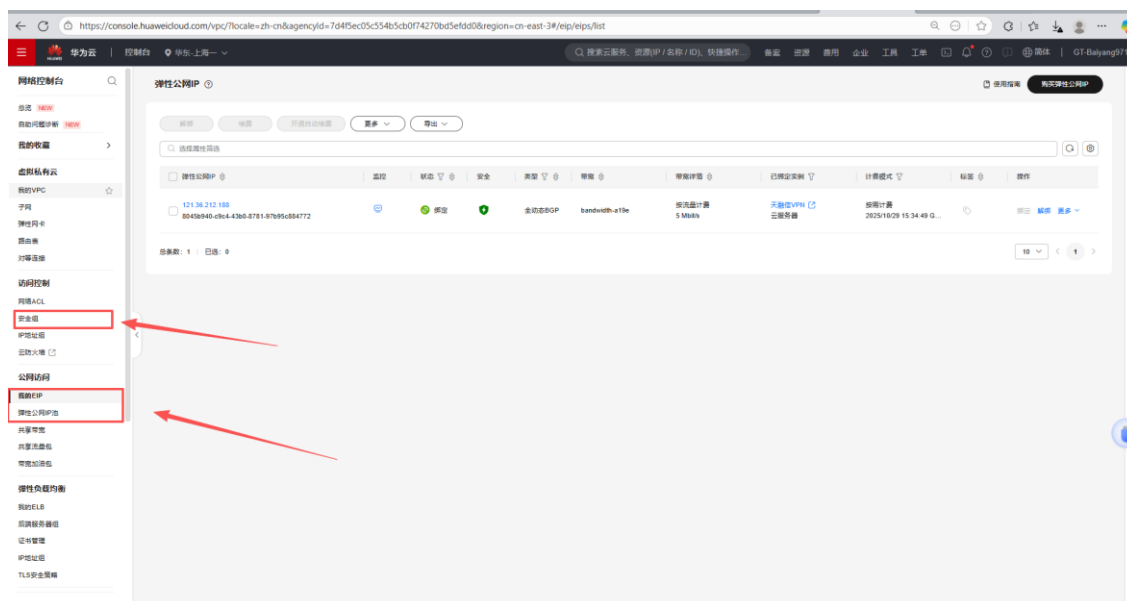


第三步：使用默认账号密码登录到云防火墙，执行“network interface show”命令，查看是否成功获取到 ip。如下图，则代表部署成功。

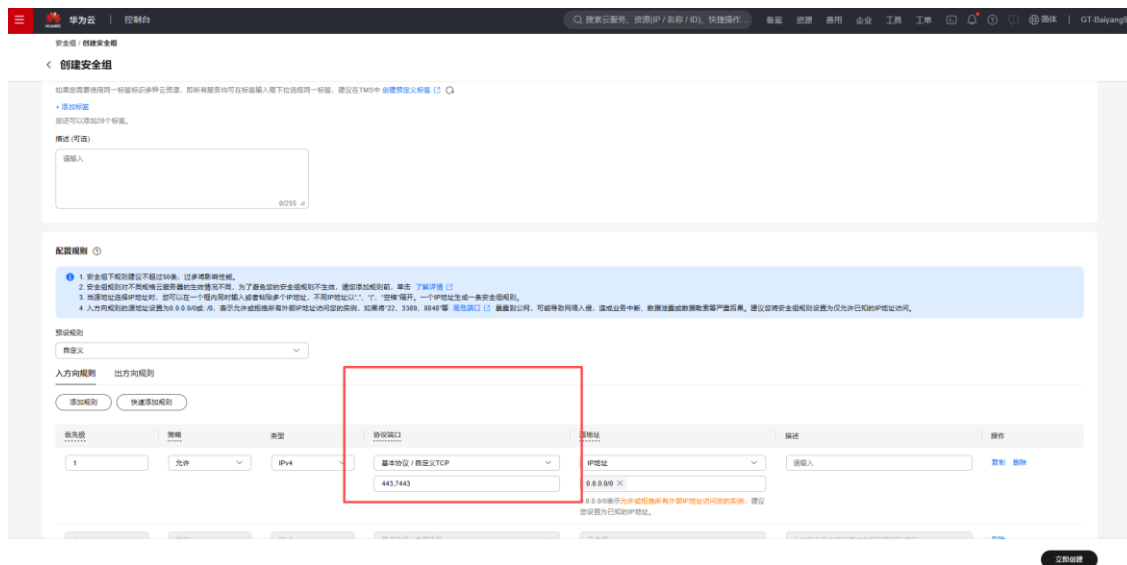


3.1.5. 配置网络和安全组

第一步点击进入网络控制台，点击“安全组”打开安全组页面，再次点击“添加入方向规则”。



第二步：配置放行“443”、“7443”端口。其中 443 为云防火墙的管理端口，7443 为授权端口，其余业务端口可按需放行。

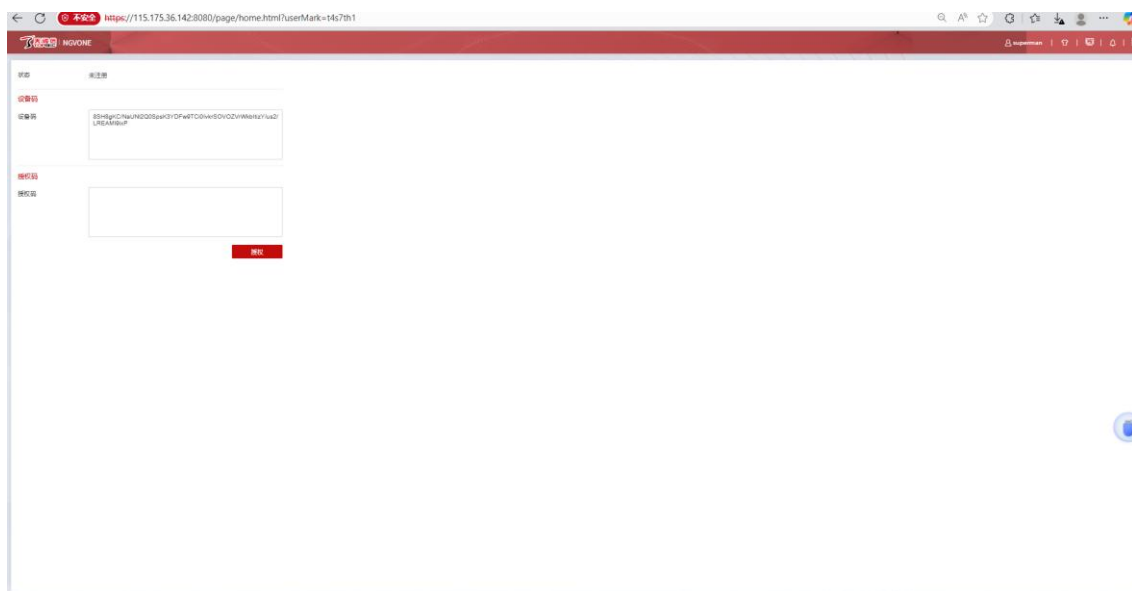


3.1.6. 设备登录

第一步：使用公网地址登录所部署的安全网元，登陆方式：<https://x.x.x.x:端口>。



第二步：设备登录成功。



4. 设备授权

4.1. 云安全管理平台授权

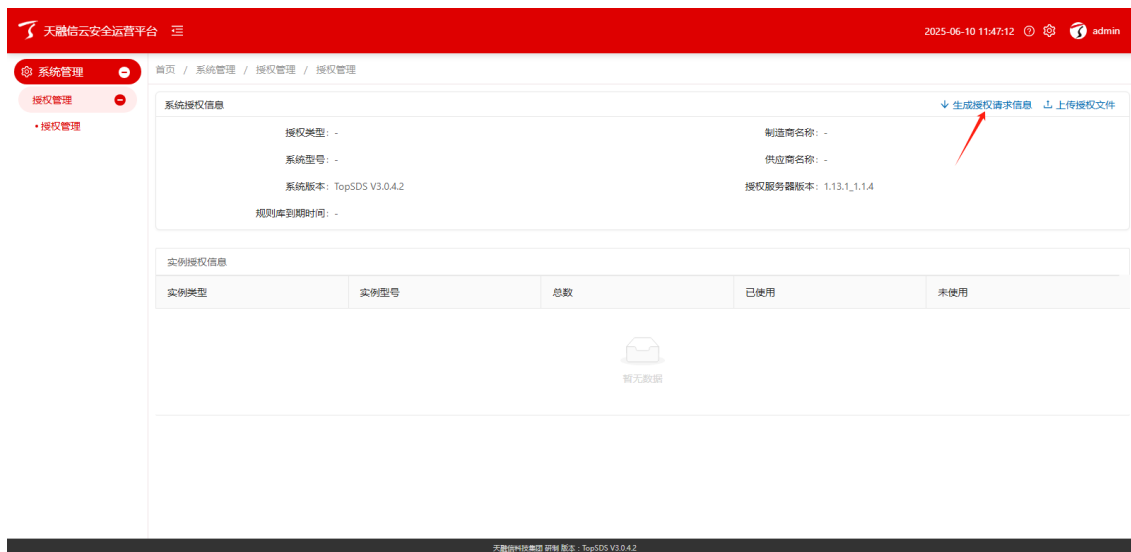
授权前请务必确保：云安全管理平台与安全网元 7443 端口双向互通。

4.1.1. 平台部署

请参照第3章节各个云平台部署流程，将云安全管理平台镜像按相同方式部署。

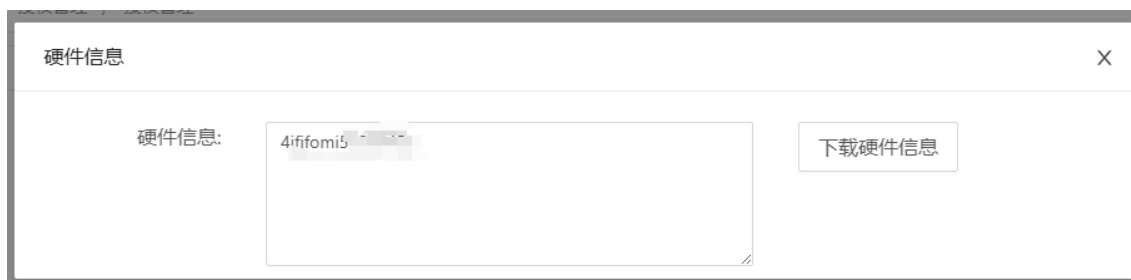
4.1.2. 授权申请

第一步：登录云安全管理平台，选择【授权管理】，点击【生成授权请求信息】。



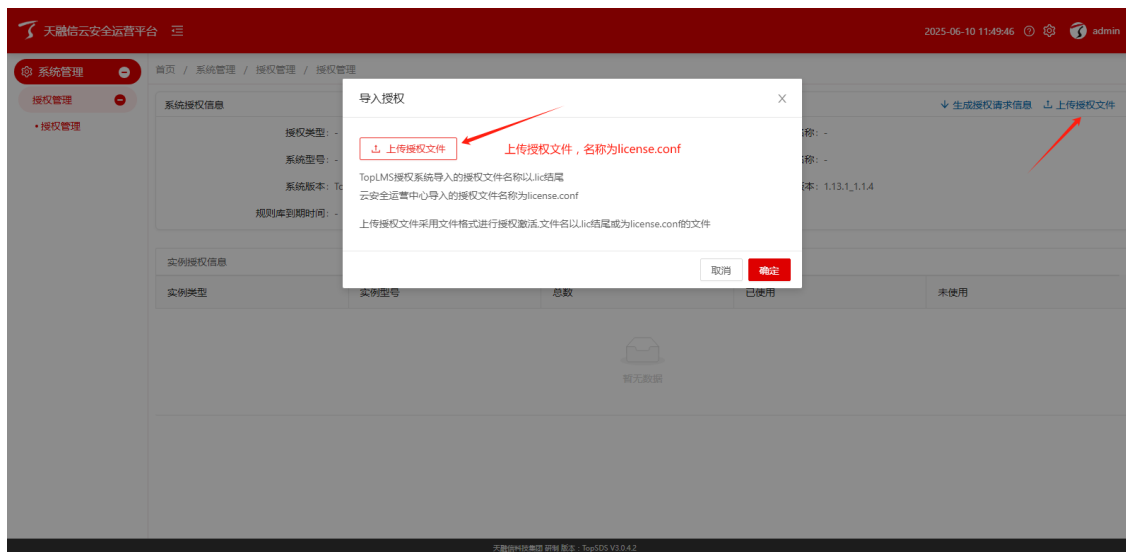
第二步：获取硬件信息码，用于后续授权申请。

请按照天融信公司流程申请所需授权，授权申请流程与问题可联系云安全推广部。



4.1.3. 授权导入

第一步：登录云安全管理平台，选择【系统管理】→【授权管理】→【上传授权文件】，导入即可。



4.1.4. 下发授权

第一步：创建租户，在【租户管理】页面添加租户，按照提示信息完成名称、密码、邮箱等填写。

添加

* 租户名称 ②: 部署指导

* 密码:

* 确认密码:

* 手机号: 13.....

* 邮箱: topsec_.....

姓名:

单位名称:

取消 确定

第二步：实例激活，在【租户管理】-【租户服务】页面，点击实例激活，填写云防火墙的地址、实例名称(可以自定义)、租户名称、实例类型、版本等信息，最后点击确定完成激活。

实例激活

X

* IP : 192.1

* 实例名称 : 云防火墙

* 租户名称 : 部署指导

* 实例类型 : 下一代防火墙

* 版本 : 高级版 → 此处注意按需选择

平台 : topsec 1.0.0

区域 :

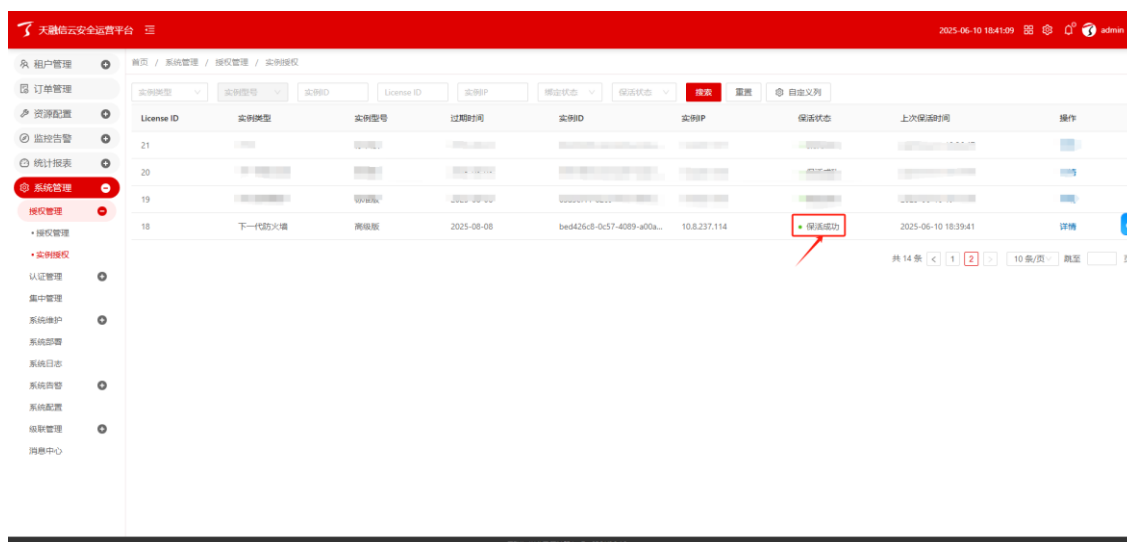
实例激活所需时间较长, 请耐心等待

取消

确定

第三步：检查状态，激活后网元会自动重启，重启后登录网元的 web 页面，在【**首页**】【**系统信息**】可以看到租约信息。同时在云安全管理平台【**系统管理**】-【**授权管理**】-【**实例授权**】可以看到此网元的保活状态，如果为保活成功，则说明授权激活成功。





4.2. License-Controller 授权

使用 License-Controller 方案，具体以版本支持情况为准，详细联系客服咨询。

5.基础配置指导

5.1. Web 应用防火墙

5.1.1. 模式部署

WAF 支持流模式和代理模式，默认部署模式为流模式。云上优先采用代理模式。

5.1.1.1. 代理模式

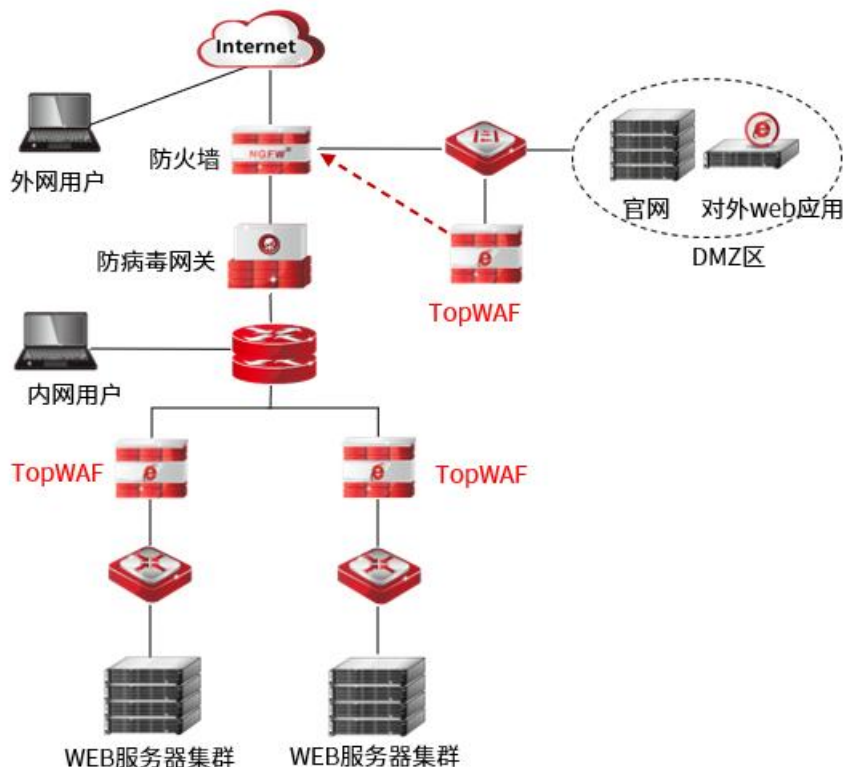
系统默认流模式，需要手动修改为代理模式。

【操作路径】：系统管理→系统设置→引擎参数，点击进入。

选择全局部署模式，下拉框选择代理模式，点击应用即可。

5.1.1.2.部署拓扑

TopWAF 部署在 Web 服务器前端。采用串联接入反向代理模式，对访问用户隐藏了 Web 服务器的真实 IP 地址，有效保障 Web 服务器安全。采用旁路部署模式，在不改变客户原有拓扑结构的前提下，实现对进出服务器的 Web 流量检测分析，同时支持与我司防火墙进行联动，及时阻断各种 Web 攻击行为，保护网站安全。



5.1.1.3.基础配置

5.1.1.3.1. 对象配置

【操作路径】：web 防护→服务器对象→服务器组，点击进入。

上游设备即待防护 web 服务器，配置服务器对应的 IP 地址和端口，多台服务器点击添加按钮继续添加。

添加

名称 * 请输入中文、数字、字母和特殊字符 - _ * .

健康检查 ☐

健康检查策略 无

服务器 *

IP地址	端口	权重	操作
		5	+ X

+ 添加 导入 IP/域名预览 1/128

确定 取消

健康检查为可选项，开启后则健康检查策略为必选项，配置正确的健康检查策略，才能开启健康检查。

添加

名称 * 请输入中文、数字、字母和特殊字符 - _ * .

健康检查类型 ☒ HTTP ☐ HTTPS ☐ ICMP ☐ TCP

异常时间间隔 * 10 秒

正常时间间隔 * 10 秒

最大失败次数 * 3

路径 * /

状态码 * 200

确定 取消

5.1.1.3.2. 策略配置

【操作路径】web 防护→服务器策略，点击进入

部署模式默认反向代理即可，配置好虚拟服务器 IP 地址和端口。云上环境，此处配置 WAF 代理接口 VPC 私有 IP 地址，不需要配置 EIP 地址。

添加

名称 *

策略

状态

☒

流量日志

☐

部署

部署模式

反向代理

类型

☒ 负载均衡 ☐ 虚拟交换

虚拟服务器 *

1.1.1.1

虚拟服务器端口 *

80

上游 *

上游web服务器

源地址池

无

调度模式 *

轮叫调度

全局重定向

☐

虚拟主机组

无

虚拟主机组取反

☐

运行模式

检测并阻断

策略

确定

取消

6. 常见问题

6.1. 无法自动获取 ip 问题

安全产品优先推荐使用网络增强型 ECS，使用其他机型可能会出现“IP 无法自动获取”、“镜像启动异常”等问题。如遇到相关问题，请联系客服及相关接口人沟通。

6.2. 授权是提示“无可授权”

7. 注意事项

- 不能选择低于最低配置建议的 ECS 规格，避免异常流量带来的性能压力。
- 注意购买云服务器的地域一定要选择和用户云业务服务器在同一地域。
- 授权完成后，需要等待一段时间，所需时间不等，但一般不超过半小时。
- 针对 https 的网站防护需要做 SSL 解密，需要将证书上传到 vWAF 上。

声明

1. 本文档所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。
2. 本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此种情况产生的差异为正常现象，产品功能或性能请以产品用户手册等资料为准。
3. 本文档中提到的信息为正常公开的信息，若因本文档或其所提到的任何信息造成或可能造成他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。