



# 云防火墙（原生版）

C100 用户使用指南

天翼云科技有限公司

## 修订记录

文档版本	发布日期	修改说明
03	2024/04/25	主要修改点： <ul style="list-style-type: none"><li>● 新增“批量管理黑白名单规则”和“批量管理防护规则”章节。</li><li>● 新增“地址簿管理”章节。</li></ul>
02	2024/03/12	主要修改点：与线上文档对齐，补充计费说明和最佳实践。
01	2022/11/30	新建文档。

---

1. 产品简介 .....	1
1.1. 产品定义 .....	1
1.1.1. 产品定义 .....	1
1.1.2. 产品功能 .....	1
1.1.3. 产品架构 .....	1
1.2. 产品优势 .....	2
1.3. 功能特性 .....	3
1.4. 术语说明 .....	5
1.5. 应用场景 .....	6
1.6. 产品使用限制 .....	7
1.7. 等保合规能力说明 .....	8
1.8. 与其他服务的关系 .....	9
1.9. 安全 .....	14
1.9.1. 审计日志 .....	15
1.9.2. 身份认证与访问控制 .....	15
1.9.3. 数据保护技术 .....	18
1.9.4. 服务韧性 .....	18
2. 计费说明 .....	20
2.1. 计费模式 .....	20



2.2. 计费项 .....	21
2.3. 续订规则 .....	22
2.3.1. 规则说明 .....	22
2.3.2. 自动续订规则 .....	23
2.4. 变配规则 .....	24
2.5. 退订规则 .....	25
3. 快速入门 .....	27
3.1. 入门指引 .....	27
3.2. 购买配额 .....	28
3.3. 开启防护 .....	34
3.4. 设置访问控制 .....	35
3.5. 设置入侵防御 .....	36
3.6. 查看防护结果 .....	37
3.7. 入门实践 .....	39
4. 用户指南 .....	40
4.1. 购买 .....	40
4.1.1. 订购 .....	40
4.1.2. 手动续订 .....	45
4.1.3. 自动续订 .....	47
4.1.4. 变配 .....	50
4.1.5. 退订 .....	51

4.2. 概览 .....	53
4.2.1. 安全防护 .....	53
4.2.2. 安全策略 .....	54
4.2.3. 防护情况 .....	54
4.2.4. 流量趋势 .....	55
4.3. 防火墙开关 .....	56
4.3.1. 同步资产 .....	56
4.3.2. 防护情况统计 .....	57
4.3.3. 防护 IP 列表 .....	57
4.4. 访问控制 .....	60
4.4.1. 防护规则概述 .....	60
4.4.2. 黑名单规则 .....	61
4.4.3. 白名单规则 .....	63
4.4.4. 外对内防护规则 .....	65
4.4.5. 内对外防护规则 .....	68
4.4.6. 批量管理黑白名单规则 .....	71
4.4.7. 批量管理防护规则 .....	74
4.5. 入侵防御 .....	78
4.5.1. 防护配置 .....	78
4.6. 日志审计 .....	79
4.6.1. 访问控制日志 .....	79



4.6.2. 入侵防御日志 .....	80
4.6.3. 流量日志 .....	81
4.6.4. 操作日志 .....	81
4.7. 设置中心 .....	83
4.7.1. 配额管理 .....	83
4.7.2. 地址簿管理 .....	84
5. 最佳实践 .....	94
5.1. 云防火墙最佳实践 .....	94
5.2. 配置访问控制策略最佳实践 .....	96
6. 常见问题 .....	98
6.1. 产品类 .....	98
6.2. 计费类 .....	103
6.3. 购买类 .....	103
6.4. 操作类 .....	104
6.5. 系统类 .....	104

# 1. 产品简介

---

## 1.1. 产品定义

### 1.1.1. 产品定义

云防火墙（原生版）（CT-CFW, Cloud Firewall）是一款云原生的云上边界网络安全防护产品，可提供统一的互联网边界管控与安全防护，并提供业务整体情况可视化、日志审计和分析等功能，帮助您完成网络边界防护与等保合规。

### 1.1.2. 产品功能

**访问控制：**可统一管理互联网访问控制策略（南北向），提供流量可视、访问控制、入侵防御等功能，全面保护用户的网络安全。

**入侵防御：**内置复合威胁检测引擎，支持对互联网上的恶意流量、DDOS 攻击，漏洞利用等攻击行为进行入侵防护，并提供精准的漏洞虚拟补丁，智能阻断入侵风险。

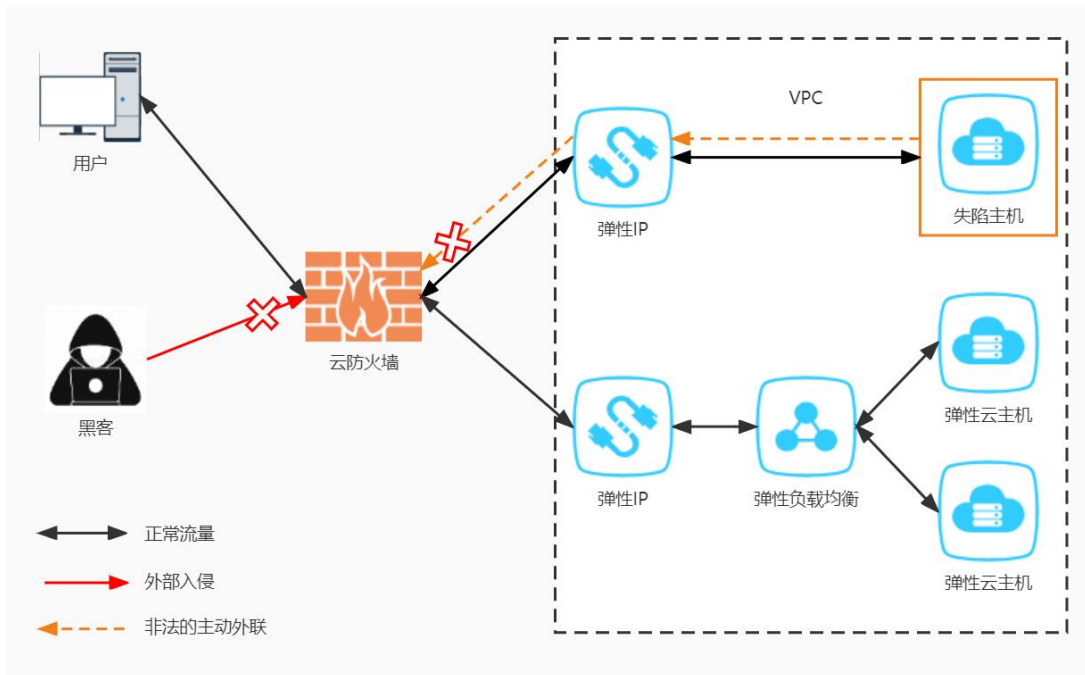
**流量可视：**提供全面的用户业务流量可视化，实现网络访问可视，网络会话可视，网络行为可视，帮助用户全面感知网络情况。

**日志审计：**为用户全面记录入侵防御日志、访问控制日志、流量日志和操作日志，帮助用户完成等保合规要求。

### 1.1.3. 产品架构

云防火墙（原生版）整体架构主要包括 3 个部分，分别为中央管理平台、南北向流量控制模块和日志平台。

- **中央管理平台：**提供策略规则的编辑和下发能力，并展示安全整体情况，为您提供可视化平台。
- **南北向流量控制模块：**主要用于实现互联网到主机间的访问控制，支持 4-7 层访问控制。
- **日志平台：**存放入侵防御日志、访问控制日志、流量日志和操作日志，并提供查询分析能力。



## 1.2. 产品优势

### 无需部署，使用便捷

云原生防火墙，可实现云上资产自动识别和防火墙一键开关。

### 独享防护，稳定可靠

每个 VPC 独享一套主备防火墙实例，防护性能稳定可靠。

### 灵活扩展，按需使用

带宽、EIP 等关键性能规格可灵活扩展，满足大流量的安全防护。

### 访问控制，能力丰富

支持基于五元组、IPS 设置、黑白名单设置访问控制。





## 1.3. 功能特性

天翼云云防火墙（原生版）产品是一款云平台 SaaS 化的防火墙，保护您的网络边界安全，主要包含以下功能：

### 概览

防火墙防御能力总览，包括安全防护、防护情况、安全策略和流量趋势。

- 安全防护展示了互联网边界防火墙的防护总体情况，包括已开启和未开启防护的 IP。
- 防护情况展示了防护的总体情况，包括入侵防御拦截数和访问控制拦截数。
- 安全策略展示了客户配置的访问控制策略的情况，分别为外->内规则数、内->外规则数、黑名单规则数、白名单规则数。
- 流量趋势展示了流量最近一段时间的入方向流量趋势和出方向流量趋势。

### 防火墙开关

目前支持互联网边界防火墙，为需要防护的 IP 资产进行开启或关闭防护。

- 公网 IP 统计了用户已开启和未开启防护的 IP，可用授权展示已经购买的云防火墙配额数。
- 防护列表展示用户所有的 EIP，列表包括公网 IP（实例名称、ID）、虚拟私有云（vpc 名称、vpc 网段）、绑定资产类型、绑定资产（资产名称、ID）、防火墙状态、配额情况和操作。

#### 说明：

可以进行 IPv4/IPv6 的切换，并可根据资产类型、防火墙状态、公网 IP 和虚拟私有云进行筛选，对于已经购买配额的 EIP，可进行开启防护和关闭防护。

### 访问控制

主要是针对互联网边界的访问和外联，基于五元组、黑名单、白名单去做 ACL 控制，分为放行、阻断两种方式。



- 访问控制规则分为外->内规则数、内->外规则数、黑名单规则数、白名单规则 4 类，可以根据需要分别进行配置。
- 其中，黑名单规则优先级最高，其次是白名单规则，最后是外对内规则和内对外规则。

说明：

- 其中访问控制规则包含 IP 地址、端口、协议、应用、动作等字段，其中 IP 地址类型为必填，默认为 IPv4。
- 源 IP/目的地址和子网掩码为必填；端口为必选，若填写时，需在 1~65535 之间进行填写。
- 协议类型、应用和动作为必选，协议类型为 TCP 时，应用可选择所有应用类型。
- 协议类型为 UDP、ICMP、Any 时，应用可选择 ANY，动作可选择放行或阻断，默认为阻断。
- 优先级默认为最后，也可以选择最前或移动至选中规则后。启用状态默认为打开，用户也可以选择关闭。
- 黑白名单规则包含地址方向、名称、IP 地址，地址方向、名称等字段，IP 地址和子网掩码为必填。

## 入侵防御

支持入侵防御功能并同步进行智能阻断，分为观察模式和拦截模式。

- 选择“观察模式”，为检测模式，针对发现的恶意访问或网络攻击行为，只告警，不自动阻断连接。
- 选择“拦截模式”，自动拦截高置信度的网络攻击或恶意访问。

## 日志审计

为您提供日志审计和行为回溯功能，展示入侵防御日志、访问控制日志、流量日志和操作日志，默认展示 7 天的日志。

- 入侵防御日志可查看云防火墙基于入侵防御“观察模式”和“拦截模式”所产生和记录的所有安全事件。
- 访问控制日志可以查看云防火墙基于用户在配置的访问控制规则所生成的规则命中记录日志。
- 流量日志可以查看互联网边界防火墙基于出站和入站所产生的南北向流量信息。



- 操作日志可以查看基于该账号内，用户的所有操作行为以及操作详情。

### 设置中心

包含配额管理，支持已订购配额的展示，支持配额订购、续订、变配和退订。

展示的范围包括正常、已到期和已退订的配额，已销毁的配额不再展示，内容包括云防火墙名称、配额规格、配额状态、虚拟私有云、可防护/已防护公网 IP 数、公网流量处理能力、配额订购时间、配额到期时间和操作。

说明：

- 只有配额状态为“正常”的才可以进行所有操作。
- 配额状态为“已到期”的可以进行续订。
- 配额状态为“已退订”的不可以进行任何操作。

## 1.4. 术语说明

### VPC

虚拟私有云（Virtual Private Cloud, VPC），为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。您可以完全掌控自己的专有网络，VPC 丰富的功能帮助您灵活管理云上网络，包括创建子网、设置安全组和网络 ACL、管理路由表、申请弹性公网 IP 和带宽等。

### 互联网边界防火墙

互联网边界防火墙主要用于检测互联网和云上资产间的通信流量，也称为南北向流量。

### 访问控制

是流量过滤规则的集合，通过防火墙的访问控制功能可以对内网的计算机进行访问限制，比如限制访问的 Internet 网站，限制使用的端口号，这样可以保证局域网的安全性。

### 黑名单规则



访问控制规则的一种。在“访问控制->互联网边界规则->黑名单规则”中配置成功后，可对配置地址的入或出通信流量进行阻断。

### **白名单规则**

访问控制规则的一种。在“访问控制->互联网边界规则->黑名单规则”中配置成功后，可对配置地址的入或出通信流量进行放通。

### **五元组**

包括源 IP 地址、目的 IP 地址、协议号、源端口、目的端口。

### **入侵防御**

主动发现外部入侵与恶意外联等未知风险，在检测到可疑事件时，提供实时的防护与告警。如果检测到攻击，入侵防御会在攻击扩散到网络的其他地方之前阻止该恶意通信。

### **主动外联访问**

主动外联访问是指云主机主动访问外部 IP 的行为，通过对主动外联访问防护，可以帮助您有效管理和控制主机外联行为。

## **1.5. 应用场景**

### **场景一：外部访问控制**

通过云防火墙（原生版）产品，对已开放公网访问的服务资产进行安全盘点，能够自动识别威胁暴露面，可一键开启入侵检测与防御。

### **场景二：主动外联管控**

对主动外联行为进行分析，评估主机失陷风险状态，并对恶意连接行为进行实时阻断，保护资产安全。

### **场景三：等保合规**

云防火墙（原生版）产品能够满足等保 2.0 二级和三级中针对边界防护、访问控制、入侵防御、安全审计等特定的等保合规检查要求。



## 1.6. 产品使用限制

### 支持的资源池

华东 1

### 产品使用条件

目前仅支持 VPC 内绑定云主机资产的 IP 南北向的防护，并且需要您在同一个 VPC 内创建一个子网掩码不大于 28 的子网网段，用于云防火墙的部署，并确保该子网中不进行任何业务配置，只用于云防火墙的部署。

### 扩展包上限

防护互联网边界的流量峰值：10Mbps-2000Mbps。

防护互联网边界公网 IP 数：20 个-1000 个。

### 访问控制规则上限

高级版套餐中，共包含最多 2000 条访问控制规则，其中外->内规则数、内->外规则数、黑名单规则数、白名单规则数分别不超过 500、500、500、500 条。

## 1.7. 等保合规能力说明

检查项分类-安全控制点-风险等级	等保合规检查项	云防火墙 CFW 提供的对应能力说明	相关功能介绍
安全通信网络-网络架构-中	应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。	云防火墙提供访问控制机制和入侵防护能力，开启防护后能够自动阻断互联网与 VPC 之间的威胁访问，为用户提供自动的边界防护能力	入侵防护 访问控制
安全区域边界-边界防护-高	应能够对内部用户非授权连到外部网络的行为进行限制或检查。	云防火墙提供南北向访问控制功能，检查外部网络连接到的内部的所有通信和内部用户连接到外部网络的通信，阻断双向非授权访问行为，保证受保护的内部网络与外部网络之间的通信在受控接口内进行通信。	访问控制
安全区域边界-边界防护-中	应能够对非授权设备私自联到内部网络的行为进行限制或检查。	云防火墙提供南北向访问控制功能，检查外部网络连接到的内部的所有通信和内部用户连接到外部网络的通信，阻断双向非授权访问行为，保证受保护的内部网络与外部网络之间的通信在受控接口内进行通信。	访问控制
安全区域边界-边界防护-中	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	云防火墙提供南北向访问控制功能，检查外部网络连接到的内部的所有通信和内部用户连接到外部网络的通信，阻断双向非授权访问行为，保证受保护的内部网络与外部网络之间的通信在受控接口内进行通信。	访问控制
安全区域边界-入侵防范-高	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。	云防火墙实现对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截。	入侵防护
安全区域边界-入侵防范-高	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。	云防火墙实现云上资产对外流量的主动外联、失陷感知等出方向流量分析和攻击防护及访问控制。	入侵防护
安全区域边界-入侵防范-中	当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	云防火墙提供对业务流量中的攻击行为的检测和记录，并能根据策略设置提供攻击流量阻断功能，记录风险级别、事件名称、源 IP、目的 IP、方向、判断来源、发生时间和动作。	入侵防护
安全区域边界-访问控制-高	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下受控接口拒绝除允许通信外的所有通信。	云防火墙提供默认拒绝所有通信的访问控制策略，只允许通行策略相关会话通信。	访问控制
安全区域边界-	应删除多余或无效的访问控制规则，优化访问	云防火墙提供流量记录功能，能够记录所有防火	访问控制

检查项分类-安全控制点-风险等级	等保合规检查项	云防火墙 CFW 提供的对应能力说明	相关功能介绍
访问控制-中	控制列表，并保证访问控制规则数量最小化。	墙的通信会话行为，可通过对防火墙网络通信判断访问规则的有效性，从而实现访问控制规则最小化。	
安全区域边界-访问控制-高	应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许或拒绝数据包进出。	云防火墙实现对进出访问控制策略进行严格设置。访问控制策略包括源类型、访问源、目的类型、目的、协议类型、目的端口、应用协议、动作、描述和优先级。	访问控制
安全区域边界-访问控制-中	应根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。	支持根据 FTP 等会话的状态信息设置对会话的允许/拒绝访问能力，控制粒度为端口级。	访问控制
安全区域边界-访问控制-中	应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	支持 DNS 等应用协议和下载等应用内容进行访问控制。	访问控制
安全区域边界-安全审计-高	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	云防火墙提供日志审计功能，可以记录所有流量日志、访问控制日志、入侵防护日志和操作日志。	日志审计
安全区域边界-安全审计-中	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	云防火墙提供日志记录事件功能，包括：时间、告警名称、攻击类型、源/目 IP 字段，等级等。	日志审计
安全区域边界-安全审计-中	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	云防火墙提供日志分析功能，默认保存 7 天的数据，同时还支持修改存储时长至 180 天。	日志审计
安全区域边界-安全审计-中	应对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	云防火墙提供日志分析功能，记录所有流量访问日志，默认保存 7 天的数据，同时还支持修改存储时长至 180 天。	日志审计

## 1.8. 与其他服务的关系

### 与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称 IAM）为云防火墙服务提供了权限管理的功能。用户在天翼云注册后自动创建主用户，该用户对其所拥有的资源具有完全的访问权限，拥有重置用户密码、分配用户等权限。用户可以通过为子用户配置不同的角色分配访问云防火墙（原生版）不同的权限。

云防火墙（原生版）角色包含 admin 角色和 viewer 角色，其中 admin 角色拥有全局权限，可以使用云防火墙（原生版）的全部功能。viewer 角色只拥有可读权限，只能查看云防火墙（原生版）相关数据，不能进行配置操作。

### 与 Web 应用防火墙（原生版）的区别

Web 应用防火墙（原生版）针对 Web 业务防护，主要应用于对七层应用流量进行防护，其防护对象为域名相关的网站，主要防护 web 攻击，通常在用户部署公网 Web 业务时，需要开启 Web 应用防火墙对网站进行防护，对非 Web 类业务没有防护能力，且只防护由外对内的攻击，对业务的恶意主动外联没有监测和防护能力。

云防火墙（原生版）包含全部业务防护，主要应用于对四层网络流量的防护和访问控制，其防护对象为用户的 IP，支持对 Web 漏洞的基础防护以及其他网络层的攻击行为，同时还支持内对外的主动外联流量检测。支持失陷主机和恶意外联的自动拦截。通常在用户开通互联网访问时需要部署，是网络访问基础的防护设备。

具体区别对比如下表：

类别	云防火墙	Web 应用防火墙
产品定义	云防火墙（原生版）（CT-CFW, Cloud Firewall）一款云原生的云上边界网络安全防护产品，可提供统一的互联网边界管控与安全防护，并提供业务整体情况可视化、日志审计和分析等功能，帮助您完成网络边界防护与等保合规	Web 应用防火墙（原生版）（CT-WAF, Web Application Firewall）为用户 Web 应用提供一站式安全防护，对 Web 业务流量进行智能全方位检测，有效识别恶意请求特征并防御，避免源站服务器被恶意入侵，保护网站核心业务安全和数据安全
防护对象	IP（弹性公网 IP、内网 IP 等）	域名
网络层级	四层	七层
应用场景	边界网络防护	Web 业务安全防护
核心技术	ACL 访问控制、DPI 深度包检测、IPS 入侵检测技术	HTTP 协议解析、web 攻击检测
安全能力	支持外部访问控制和主动外联管控，能够检测攻击者对用户网络发起的攻击，同时也能对用户网络主动外联行为进行分析，阻断由内而外的恶意连接行为，保护用户的资产安全	集成机器学习检测引擎，支持专家经验特征与语义特征，有效检测 SQL 注入、XSS 等基于形式语言的攻击类型，对 OWASP 常见攻击类型进行了良好覆盖





Web 应用防火墙建议使用场景：

当用户部署了对外提供服务的 Web 应用时，建议用户购买 Web 应用防火墙，以便能够保护所部署 Web 服务的安全。

注意：

无论所部署的 Web 服务是否位于天翼云上，都可以购买天翼云 Web 应用防火墙（原生版）对用户的 Web 服务提供防护，天翼云 Web 应用防火墙（原生版）提供全球级服务，能够为用户任意位置的 Web 服务提供全面的 Web 安全保护。

云防火墙建议使用场景：

当用户在天翼云上购买了弹性云主机时，建议购买云防火墙，以便能够保护用户云上弹性云主机的安全。

#### 注意：

天翼云云防火墙仅能保护部署在天翼云内的弹性云主机网络安全，对于在其他位置的主机和网络设备，因其网络流量未流经天翼云，故天翼云云防火墙无法保护其网络安全。

### 与 VPC 的关系

VPC 是基于天翼云创建的自定义私有网络，为弹性云主机提供一个逻辑上完全隔离的专有网络，您还可以在 VPC 中定义安全组、IP 地址段、带宽等网络特性。用户可以通过 VPC 方便地管理、配置内部网络，进行安全、快捷的网络变更，详细内容请参见虚拟私有云。云防火墙目前仅支持 VPC 内绑定云主机资产的 IP 南北向的防护，并且需要您在同一个 VPC 内创建一个子网掩码不大于 28 的子网网段，用于云防火墙的部署，并确保该子网中不进行任何业务配置，只用于云防火墙的部署。

### 与弹性 IP 的关系

弹性 IP (Elastic IP, EIP) 是可以独立申请的公网 IP 地址，包括公网 IP 地址与公网出口带宽服务。可以与云主机、物理机、负载均衡、NAT 网关等云产品动态绑定和解绑，实现云资源的互联网访问，详情请参见弹性 IP。云防火墙会自动同步用户账户下的弹性 IP 资产，并显示其防护状态。用户可自主决策是否对弹性 IP 开启安全防护，首次购买后，您会自动进入防火墙控制台页面，同时防火墙自动为您同步资产，同步完成后，公网 IP 默认处于关闭防护状态，需要您自己“开启防护”，并去配置相关的规则。公网 IP 统计了您已开启和未开启防护的公网 IP，对应防火墙状态中的“已防护”和“未防护”状态，未防护的统计所有绑定资产类型对应的公网 IP。可用授权展示已经购买的云防火墙配额数，每个配额可防护一个 VPC，您可以为该 VPC 中的所有 IP 开启防护。云防火墙 (CFW) 与 EIP 关系如下图：



## 1.9. 安全

## 1.9.1. 审计日志

审计日志是记录云防火墙的用户活动、权限管理和数据访问等信息的日志，通过审计日志可以帮助用户完成对云防火墙可靠性、可用性监测，用户可以通过审计防火墙的日志观测防护墙的操作记录、防火墙的运行记录、防火墙的资源使用情况等，审计日志对于系统的合规性和安全性具有重要作用。天翼云云防火墙（原生版）已生成防火墙操作日志，记录操作发生时间、操作账号、危险等级、操作行为等信息为用户审计防火墙操作行为提供基础日志数据，可以帮助用户对防火墙使用情况，配置情况等审计与监测，以保证对防火墙的操作都能够被审查。

### 说明：

审计日志存储与数据日志存储是分开存储在不同的地方，以保证审计日志不会因数据日志的循环而被删除，审计日志默认存储 180 天，以保证用户业务的可审计性。

## 1.9.2. 身份认证与访问控制

### 用户身份、角色、策略说明

用户在天翼云注册后自动创建主用户，该用户对其所拥有的资源具有完全的访问权限，拥有重置用户密码、分配用户等权限。若需多人共同使用天翼云资源，为确保账号安全，建议创建子用户来进行日常管理工作。子用户是由拥有 IAM 权限的用户在用户管理中心创建，创建初期是没有任何权限，需要先创建用户组授予相应的策略并把创建的用户加到用户组，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

根据授权分为角色、委托和策略。

角色：权限控制针对所有天翼云用户，IAM 需要识别访问者的角色身份并赋予相应的委托权限策略。

委托：包括用户和用户之间的委托等操作用户的资源属于委托的范畴。

策略：是描述一组权限集的语言，它可以精确地描述被授权的资源集和操作集，通过策略，用户可以自由搭配需要授予的权限集。通过给用户组授予策略，用户组中的用户就能获得策略中定义的权限。

## 云防火墙的身份认证与访问控制

天翼云云防火墙（原生版）已经对接了统一身份认证服务（Identity and Access Management, IAM）服务。可通过 IAM 的权限定义可实现对云资源权限的访问控制。通过 IAM，可以将用户加入到一个用户组中，并用策略来控制他们对云资源的访问范围，也可以将用户加入到企业项目中，为用户赋予企业项目的权限。

## 云防火墙角色

云防火墙角色如下表

角色名称	类型	作用范围	描述
CFW admin	系统默认角色	全局	全局策略，拥有所有读写权限
CFW viewer	系统默认角色	全局	只读策略，拥有只读权限

## CFW admin 策略内容

```
{
  "Version": "1.0",
  "Statement": [
    {
      "effect": "Allow",
      "action": [
        "cfw:agent:download",
        "cfw:agent:query",
        "cfw:app:query",
        "cfw:app:reload",
        "cfw:blackWhitePolicy:add",
        "cfw:blackWhitePolicy:delete",
        "cfw:blackWhitePolicy:query",
        "cfw:blackWhitePolicy:update",
        "cfw:dpi:query",
        "cfw:firewall:add",
        "cfw:firewall:delete",
        "cfw:firewall:destroy",
        "cfw:firewall:query",
        "cfw:firewall:update",
        "cfw:flowLog:add",
        "cfw:flowLog:query",

```

```
"cfw:heartBeat:query",
"cfw:igw:query",
"cfw:ipsRule:query",
"cfw:ipsRule:update",
"cfw:logSetting:query",
"cfw:logSetting:add",
"cfw:operationLog:query",
"cfw:whiteList:add",
"cfw:whiteList:delete",
"cfw:whiteList:update",
"cfw:whiteList:query",
"cfw:systemSecPolicy:add",
"cfw:systemSecPolicy:delete",
"cfw:systemSecPolicy:query",
"cfw:systemSecPolicy:update",
"cfw:systemVrfBind:query",
"cfw:systemVrfBind:update",
"cfw:report:query",
"cfw:report:download",
"cfw:report:update",
"cfw:report:",
"cfw:alarm:query",
"cfw:alarm:update",
"cfw:notification:query",
"cfw:notification:update",
"cfw:logManager:query",
"cfw:logManager:update",
"cfw:logManager:download"
]
}
]
}
```

## CFW Viewer 策略内容

```
{
"Version": "1.0",
"Statement": [
{
"effect": "Allow",
"action": [
"cfw:agent:query",
"cfw:app:query",
```

```

"cfw:blackWhitePolicy:query",
"cfw:dpi:query",
"cfw:firewall:query",
"cfw:flowLog:query",
"cfw:heartBeat:query",
"cfw:igw:query",
"cfw:ipsRule:query",
"cfw:logSetting:query",
"cfw:operationLog:query",
"cfw:whiteList:query",
"cfw:systemSecPolicy:query",
"cfw:systemVrfBind:query",
"cfw:report:query",
"cfw:alarm:query",
"cfw:notification:query",
"cfw:logManager:query"
]
}
]
}

```

### 1.9.3. 数据保护技术

数据保护手段	简要说明
传输中的数据保护	日志数据采用安全协议 HTTPS 传输到日志服务，防止数据被窃取；用户的配置数据传输采用安全协议 HTTPS，防止数据被窃取。
配置数据完整性	CFW 会和配置管理中心检验配置一致性，实时确保配置的准确性和完整性
数据销毁机制	考虑到残留数据导致的用户信息泄露问题，保留期到期仍未续订或充值，存储在云服务中的数据将被删除，云服务资源将被释放。CFW 会清除用户数据，避免用户数据残留造成信息泄露。
数据存储安全	对静态数据进行透明加密，可以保护数据免受可以访问底层文件系统的攻击者的影响

### 1.9.4. 服务韧性

天翼云云防火墙（原生版）的管理平台、引擎、日志服务等组件均采用主备或集群方式部署，并在多个可用区部署，从而保证云防火墙服务的韧性。

- 其中管理平台采用集群式部署架构，支持服务器级别的容灾备份。



- 日志服务采用集群式部署架构，支持服务器级别的容灾备份。
- 引擎采用主备部署架构，当主设备出现故障时能够快速切换到备设备提供服务。

说明：

主备设备之间采用心跳进行状态检测，同时引擎还支持直接转发的功能，当主备设备同时出现故障时，能够将流量直接转发到用户的业务上，不影响用户的业务正常运行。任意一台服务器或者任意一个可用区故障时都不会导致云防火墙故障。

## 2. 计费说明

### 2.1. 计费模式

#### 标准资费

云防火墙（原生版）产品提供包年包月计费方式。

#### 包年包月计费

计费项	计费单位	标准资费
高级版	元/月	2800
流量扩展费用	元/Mbps/月	50
IP 扩展费用	元/个/月	50

#### 说明：

针对一次性包年付费服务，云防火墙（原生版）包年优惠价格为：1年 85 折、2年 7 折、3年 5 折。

高级版具体支持功能如下：

支持的功能	高级版
防护互联网边界的流量峰值	10Mbps-2000Mbps（可扩展）
防护互联网边界公网 IP 数	20 个-1000 个（可扩展）
互联网边界访问控制	支持外对内防护规则、内对外防护规则、黑名单、白名单各 500 条
VPC 间防火墙	不支持
入侵防御（IPS）	支持

支持的功能	高级版
日志审计	支持
日志分析	默认存储 7 天，可单独购买

## 规则

### 续订规则：

云防火墙（原生版）购买周期到期后，若未及时进行手动续订或开启自动续订，资源将到期冻结。配额冻结后，进入保留期，在保留期内展示全部历史告警数据和防护配置策略，但该防护配额自动降级为 2Mbps 的公网流量处理能力，除非客户重新订购该 VPC 的防火墙；保留期后，进行该配额的资源销毁，开启自动续订或更多信息请查看[续订规则](#)。

### 变配规则：

创建云防火墙实例后，如果当前实例配置无法满足您的业务需求，您可以修改实例规格。您可以对实例的可防护公网 IP 数、公网流量处理能力数值进行调整，升配和降配均可支持。更多信息请查看[变配规则](#)。

### 退订规则：

创建云防火墙实例后，如果当前实例配置无法满足您的业务需求，可根据需要，在符合天翼云退订规则的前提下，灵活退订配额。目前退订包含七天无理由全额退订和非七天无理由退订以及其他退订。更多信息请查看[退订规则](#)。

## 2.2. 计费项

天翼云云防火墙（原生版）根据您选择的服务版本、流量扩展项、IP 扩展项和购买时长计费。

## 2.3. 续订规则

### 2.3.1. 规则说明

#### 续订简介

购买的包年/包月云防火墙（原生版）服务到期后，将会影响服务的正常运行，若配额到期后未及时续订，或进行退订，则将被到期冻结或超期释放。

配额冻结后，进入保留期，在保留期内展示全部历史告警数据和防护配置策略，但该防护配额自动降级为 2Mbps 的公网流量处理能力，除非客户重新订购该 VPC 的防火墙；保留期后，进行该配额的资源销毁。

配额销毁后，只保留历史的配置规则。若配额到期后续费，续费周期自配额续订解冻开始，计算新的服务有效期，按照新的服务有效期计算费用。例如，客户配额 2020 年 9 月 30 号到期，10 月 11 号续订 1 个月，那么新的服务开始时间为 10 月 11 号，到期时间为 11 月 10 号。相关费用自 10 月 11 号开始计算。

注意：

- 未完成订单中的配额不允许续订，如开通中的资源、退订中的资源。
- 已退订或销毁的配额不可续订。
- 只有通过实名认证的客户，才可以执行续订操作。

## 续订方式

包年/包月云防火墙（原生版）支持的续订方式如下表所示。

续订方式	说明
手动续订	包年/包月云防火墙在购买之后支持手动续订的方式，您可以随时在云防火墙（原生版）管理控制台中的配额管理页面进行续订，续订后防火墙到期时间将自动延期到续订后的到期时间。
自动续订	包年/包月云防火墙在购买之后支持自动续订的方式，您可以随时在管理中心-订单管理-续订管理中开启自动续订，自动续订开启后云防火墙将会进行自动续订，更多说明见 <a href="#">自动续订</a> 。

## 2.3.2. 自动续订规则

### 自动续费简介

为避免由于未及时对配额采取续订操作，配额被到期冻结或超期释放，客户购买包月包年产品后，可设置开通自动续订。开通自动续订后，系统将在配额到期前自动续订，无需客户再手动操作。

### 适用范围

自动续订仅针对采用包月、包年计费模式的资源。已到期资源不支持设置/修改自动续订。

### 开通、变更、关闭自动续订

您在续订管理页可开通自动续订功能，变更自动续约周期，或关闭自动续订。

不关闭自动续订的情况下，只要预付费账户余额充足，或为后付费客户，系统将持续按设定的周期自动续订下去。

预付费您可在官网自主控制自动续订功能的开通、变更、关闭。后付费您需要客户经理协助开启自动续订权限后才可以自主管理。

### 自动续订周期

包月产品默认自动续订周期为 3 个月，包年产品默认自动续订周期为 1 年，您可按需调整自动续订周期。

### 自动续订价格

自动续订下单扣费时按当时的标准价自动续订，续订 1 年或以上可享受包年折扣。

0 元、秒杀等特价促销活动产品订购后，自动续订下单扣费时恢复标准价。

预付费您暂不支持代金券支付，仅支持余额支付，您需确保账户余额充足。

### 自动续订扣费规则

支付方式及支付时间：将在资源到期前 10 天和前 7 天进行两次自动续订下单及扣费。

自动续订订单出账后不可取消。客户如有问题，可发起退订，自动续订订单的退订与退订规则保持一致，退订的同时，该资源的自动续订自动关闭。

### 自动续订和手动续订的关系

在 7 天或更短时间内到期的资源，或已到期资源，需手动续订，无法设置自动续订。

开通自动续订功能后，也可以进行手动续订。在自动续订扣费日前进行手动续订，系统将按照手动续订后的到期日期，重新计算下一次自动续订的下单时间。

## 2.4. 变配规则

创建云防火墙实例后，如果当前实例配置无法满足您的业务需求，您可以修改实例规格。您可以对实例的可防护公网 IP 数、公网流量处理能力数值进行调整，升配和降配均可支持。

- 可防护公网 IP 数可支持的规格范围是 20 个-1000 个。
- 公网流量处理能力可支持的规格范围是 10Mbps-2000Mbps。

#### 注意：

当您进行降配时，降配后的 IP 规格不能小于该 VPC 内正在防护的公网 IP 数，且需要分步降配可防护公网 IP 数和公网流量处理能力。

## 2.5. 退订规则

客户（天翼云您）可根据需要，在符合天翼云退订规则的前提下，灵活退订配额。目前退订包含七天无理由全额退订和非七天无理由退订以及其他退订。

### 七天无理由全额退订

新购配额（不包含进行了续订等操作的资源）在满足以下全部条件的前提下，享受七天无理由全额退订：

- 在资源开通的 7 天内发起退订；
- 发起退订操作的账号（“退订账号”）当年的七天无理由全额退订次数不超过 3 次（每账号每自然年享有 3 次七天无理由全额退订次数，从每年的 1 月 1 日开始计算）；
- 同一您累计使用的七天无理由全额退订次数不超过 24 次。其中，同一您是指：根据不同天翼云账号在注册、登录、使用中的关联信息，关联信息相同天翼云判断其实际为同一您。关联信息举例：同一名称、同一邮箱、同一负责人证件、同一手机号、同一设备、同一 IP 地址等（包括已注销的账号）。**客户同意天翼云使用上述信息核查同一您情况。**

成套资源退订属于退订一个资源实例，记为 1 次退订。

#### 注意：

尽管有上述规则，客户不得利用退订规则频繁订购并退订服务，恶意占用天翼云及其他您资源。如天翼云有合理理由怀疑客户存在频繁退订恶意占用天翼云及其他您资源的，则天翼云有权取消该客户七天无理由全额退订的权利，并根据《中国电信天翼云您协议》及网站相关规则和相关服务协议约定，采取相应措施直至终止服务，并追究客户的违约责任。

### 非七天无理由退订

不符合七天无理由全额退订条件的退订，都属于非七天无理由退订。非七天无理由退订，不限制退订次数，但退订需要收取相应的使用费用和退订手续费，且不退还代金券及优惠券，但符合下文“其他退订”情形的除外。

### 其他退订



主要指因创建资源失败或资源未生效等因天翼云原因导致的您退订。该类退订不限制退订次数，实现无条件退费。

### **注意事项**

七天无理由退订仅限于新购资源的情形，若新购资源在 7 天内进行了续订或变更（包括但不限于规格升级、扩容、操作系统变更），退订时按非七天无理由退订处理，需要收取相应的使用费用和退订手续费，且不退还代金券及优惠券。

参与活动购买的云产品，如若本退订规则与活动规则冲突，以活动规则为准；活动中说明“不支持退订”的云服务资源不支持退订。

执行退订操作前，请确保退订的资源数据已完成备份或迁移，退订完成后的资源将被完全删除，且不可恢复，请谨慎操作。

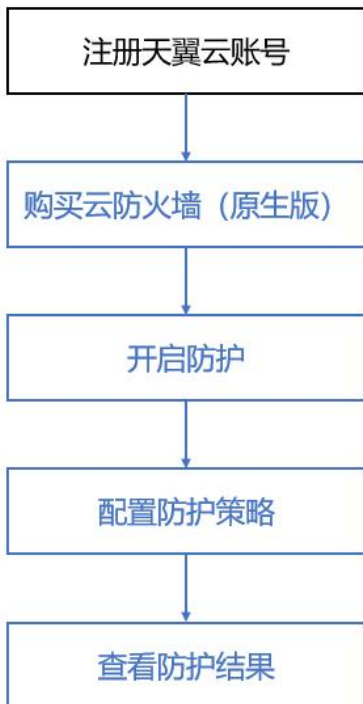


## 3. 快速入门

### 3.1. 入门指引

一款云原生的云上边界网络安全防护产品，可提供统一的互联网边界、内网 VPC 边界、主机边界管控与安全防护，并提供实时入侵防护、全流量业务可视化、日志审计和分析等功能，帮助用户完成网络边界防护与等保合规业务。

使用流程如下图：



#### 注册天翼云账号

在创建和使用云防火墙（原生版）之前，您需要先注册天翼云门户的账号，注册步骤见注册天翼云账号。

如果您拥有天翼云的账号，请跳转到下一节“开通云防火墙（原生版）”。

#### 购买云防火墙（原生版）配额

成功注册天翼云账号后，打开控制中心，切换资源池至目标资源池，选择云防火墙（原生版）产品，点击购买配额。

## 开启防护

打开云防火墙（原生版）控制台，选择防火墙开关，开启防护。

## 配置防护策略

购买成功后，打开云防火墙（原生版）控制台，配置访问控制策略和防护策略。

## 查看防护结果

策略配置成功后，查看防护结果日志，防火墙成功开启。

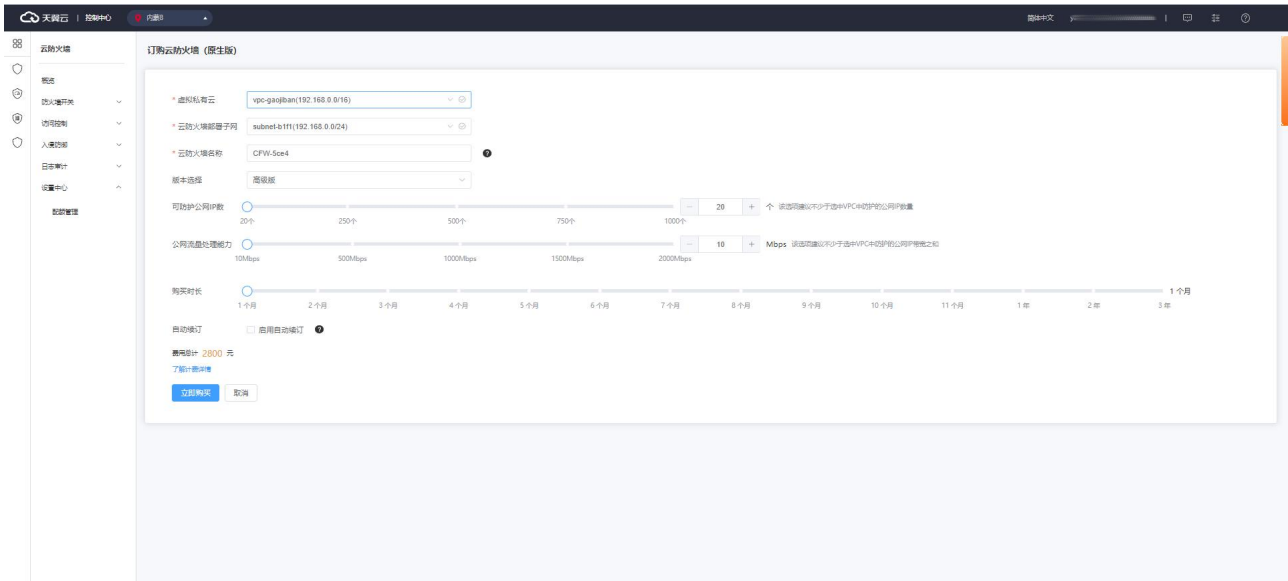
## 3.2. 购买配额

当您具备已通过实名认证的 ctyun 账号后，可以通过以下两种方式开通云防火墙（原生版）：

1. 在天翼云官网首页选择“产品->安全->网络安全->云防火墙（原生版）”。进入云防火墙（原生版）产品详情页后，选择“立即开通”，如下图所示：



进入到云防火墙（原生版）产品购买页面，如下图所示：



您需要选择虚拟私有云、云防火墙部署子网、云防火墙名称、版本、可防护公网 IP 数、公网流量处理能力和购买时长和是否自动续订。

**虚拟私有云：**该下拉选项中展示您在该地域的所有 VPC，选择您需要防护的 VPC。由于一个 VPC 只能购买一个 VPC 配额，因此已经购买配额的 VPC 不能重复进行购买。

**云防火墙部署子网：**可以下拉选择用户该 VPC 中的子网，展示该子网 ID 和子网网段。需要您在需要防护的 VPC 中创建一个子网掩码不大于 28 的子网网段，在此处进行选择，用于云防火墙的部署，并确保该子网中不进行任何业务配置，只用于云防火墙的部署。

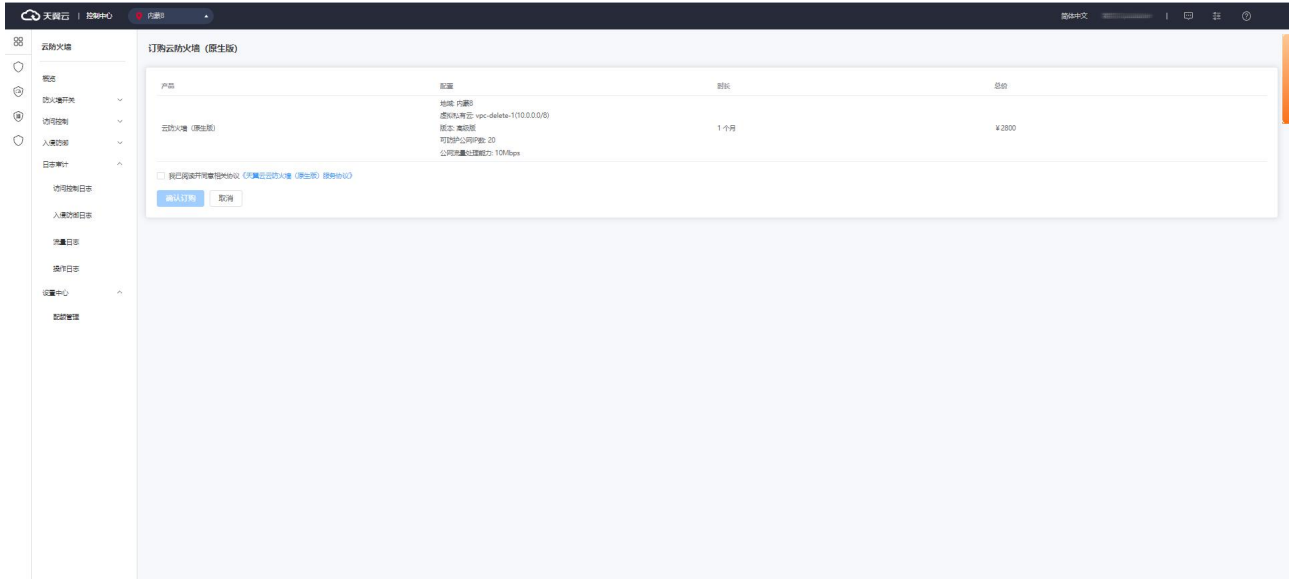
**云防火墙名称：**只能由数字、字母、-组成，不能以数字和-开头、以-结尾，且长度为 2-63 字符。

**可防护公网 IP 数：**可以单击加减号调整防护公网 IP 数，步长为 1，也可以在其中直接输入。可防护公网 IP 数的范围是 20 个-1000 个。

**公网流量处理能力：**可以单击加减号调整公网流量处理能力，步长为 5，也可以在其中直接输入。公网流量处理能力 10Mbps-2000Mbps。

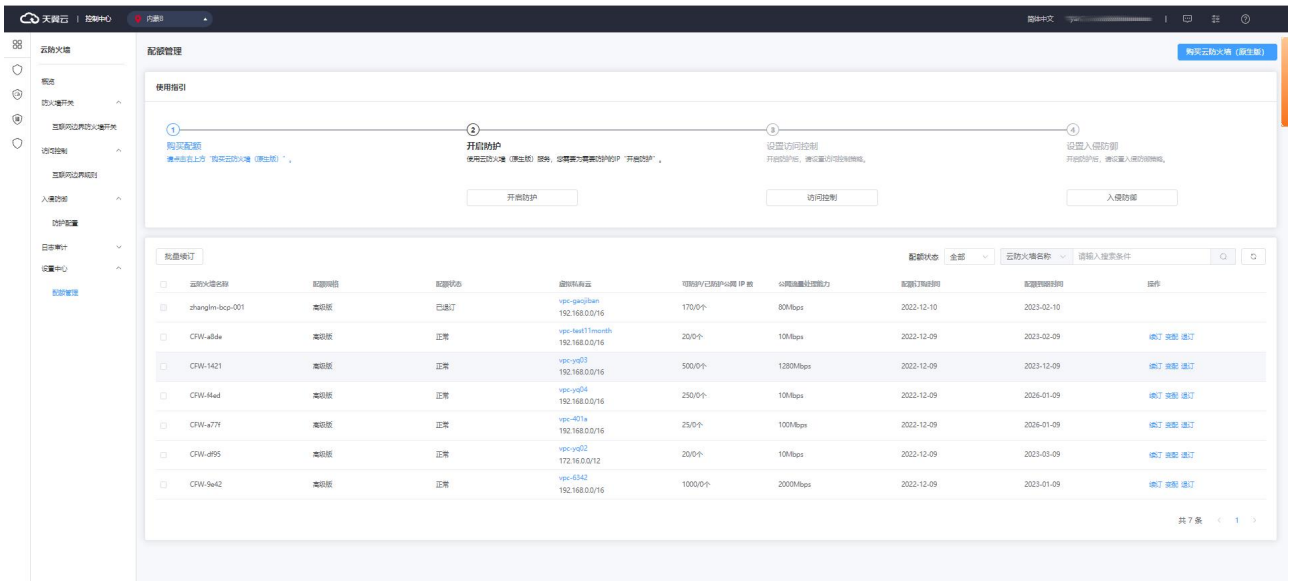
**自动续订：**按月购买自动续订周期为 3 个月，按年购买自动续订周期为 1 年。您可以在续订管理中修改自动续订周期。

以上参数均选择完毕后，勾选我已阅读并同意相关协议《天翼云云防火墙（原生版）协议》，点击“立即购买”按钮，进入如下页面：

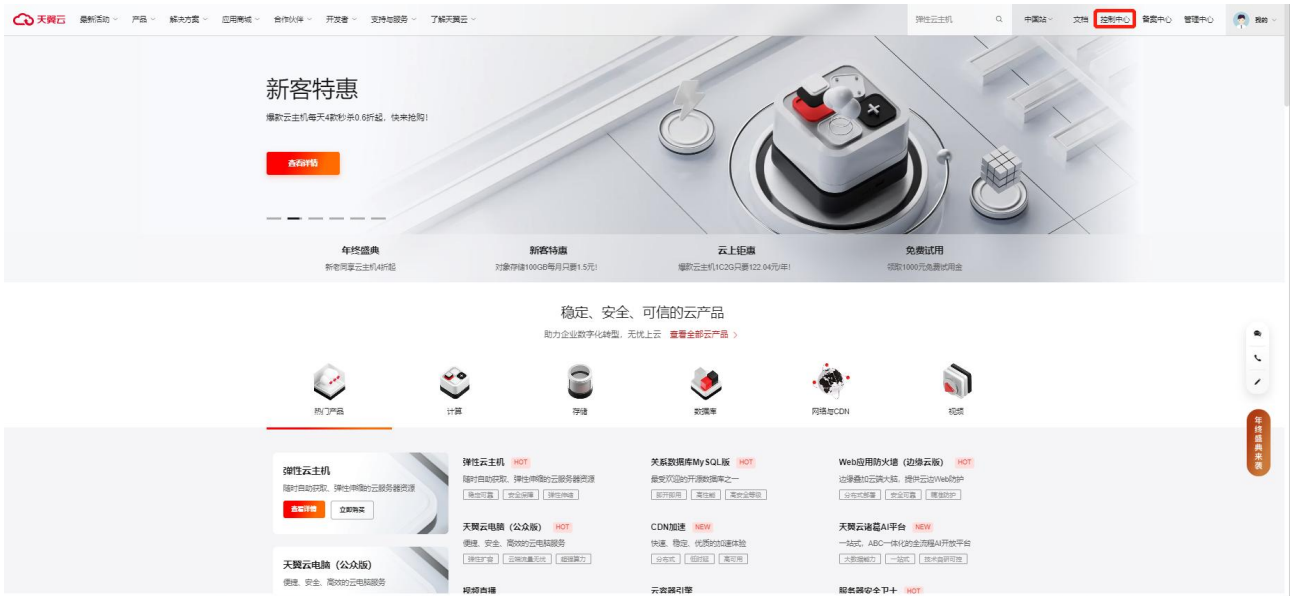


您需要确认地域、虚拟私有云、版本、可防护公网 IP 数、公网流量处理能力、购买时长和总价，确认后单击“确认订购”后即可完成任务。若未确认则单击“上一步”返回订购页面重新选择。

订购成功后即可在“配额管理”页面查看已购买的高级版配额，如下图所示：



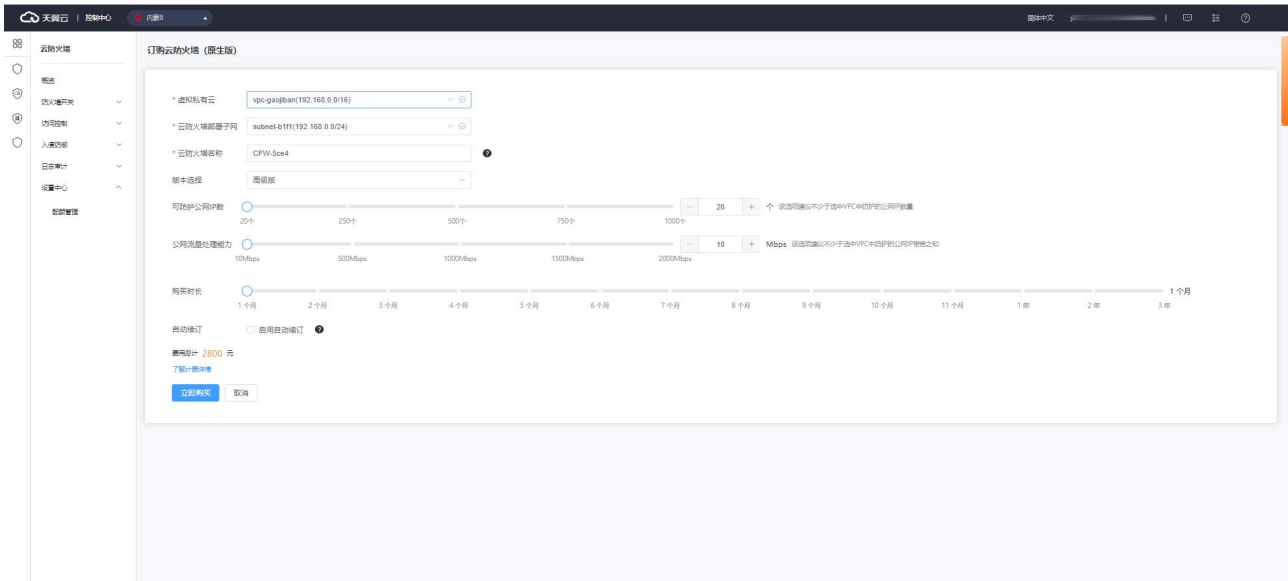
2. 在天翼云官网首页选择“控制中心”，如下图所示：



在天翼云控制台中，安全分类下，点击“云防火墙（原生版）”，



进入云防火墙（原生版）产品购买页面，如下图所示：



您需要选择虚拟私有云、云防火墙部署子网、云防火墙名称、版本、可防护公网 IP 数、公网流量处理能力和购买时长和是否自动续订。

**虚拟私有云：**该下拉选项中展示您在该地域的所有 VPC，选择您需要防护的 VPC。由于一个 VPC 只能购买一个 VPC 配额，因此已经购买配额的 VPC 不能重复进行购买。

**云防火墙部署子网：**可以下拉选择用户该 VPC 中的子网，展示该子网 ID 和子网网段。需要您在需要防护的 VPC 中创建一个子网掩码不大于 28 的子网网段，在此处进行选择，用于云防火墙的部署，并确保该子网中不进行任何业务配置，只用于云防火墙的部署。

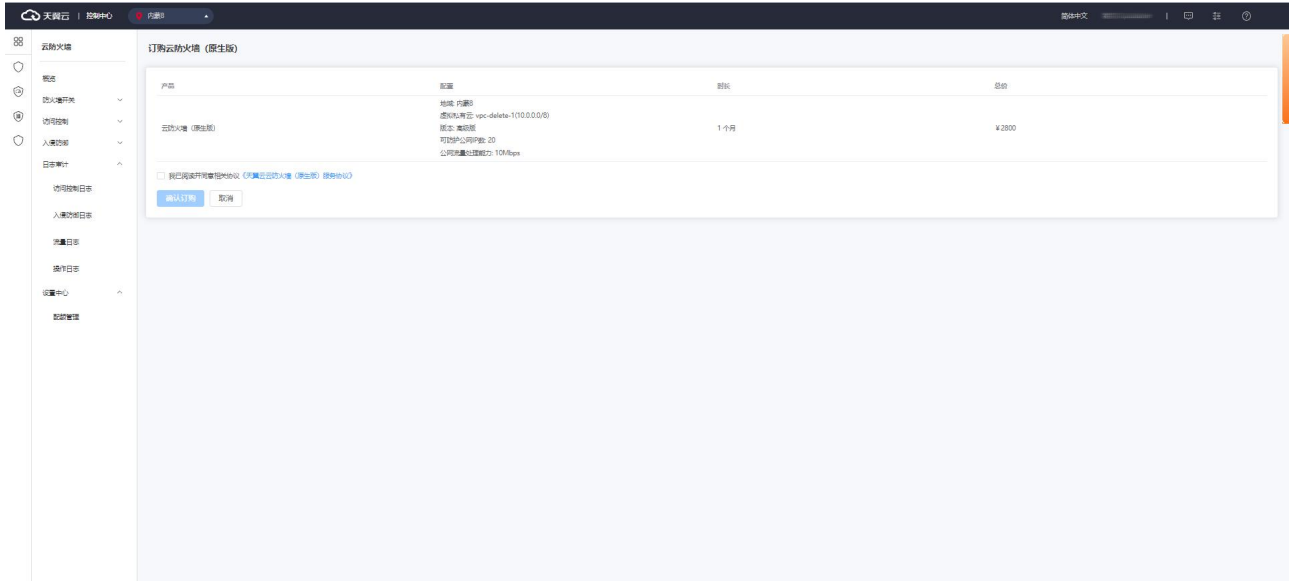
**云防火墙名称：**只能由数字、字母、-组成，不能以数字和-开头、以-结尾，且长度为 2-63 字符。

**可防护公网 IP 数：**可以单击加减号调整防护公网 IP 数，步长为 1，也可以在其中直接输入。可防护公网 IP 数的范围是 20 个-1000 个。

**公网流量处理能力：**可以单击加减号调整公网流量处理能力，步长为 5，也可以在其中直接输入。公网流量处理能力 10Mbps-2000Mbps。

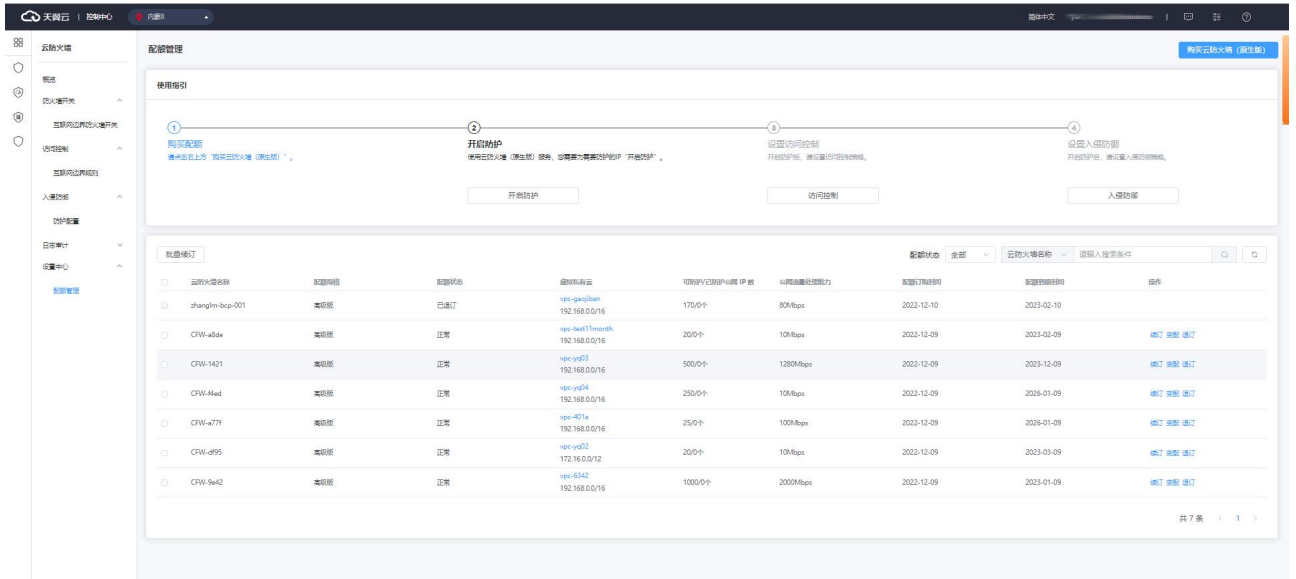
**自动续订：**按月购买自动续订周期为 3 个月，按年购买自动续订周期为 1 年。您可以在续订管理中修改自动续订周期。

以上参数均选择完毕后，勾选我已阅读并同意相关协议《天翼云云防火墙（原生版）协议》，点击“立即购买”按钮，进入如下页面：



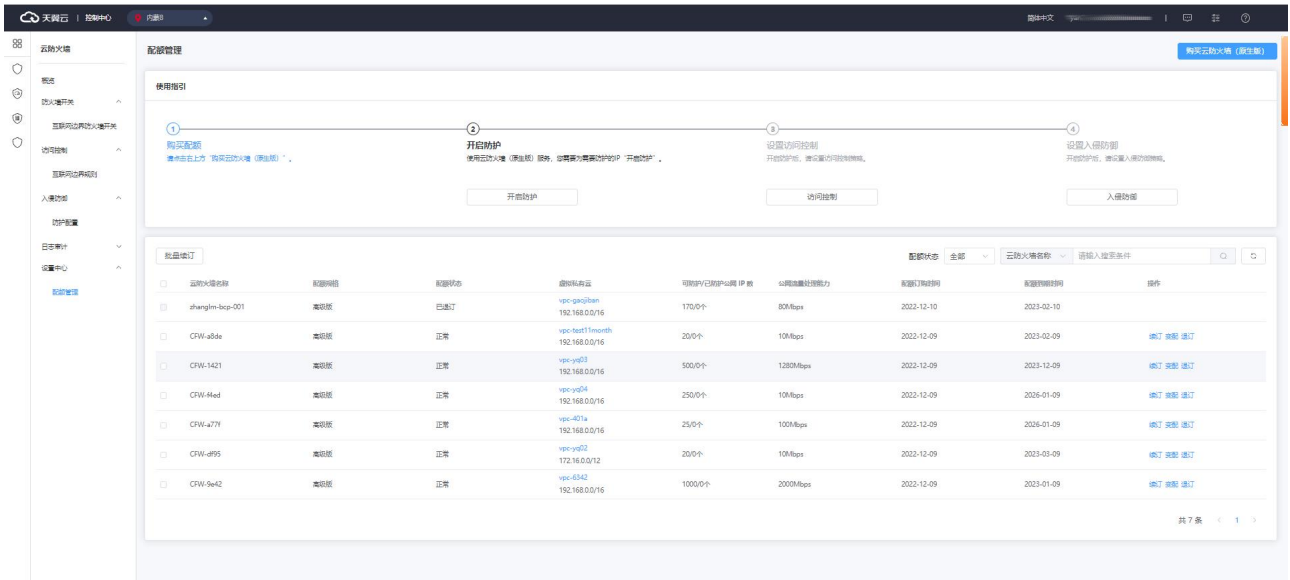
您需要确认地域、虚拟私有云、版本、可防护公网 IP 数、公网流量处理能力、购买时长和总价，确认后单击“确认订购”后即可完成订购。若未确认则单击“上一步”返回订购页面重新选择。

订购成功后即可在“配额管理”页面查看已购买的高级版配额，如下图所示：

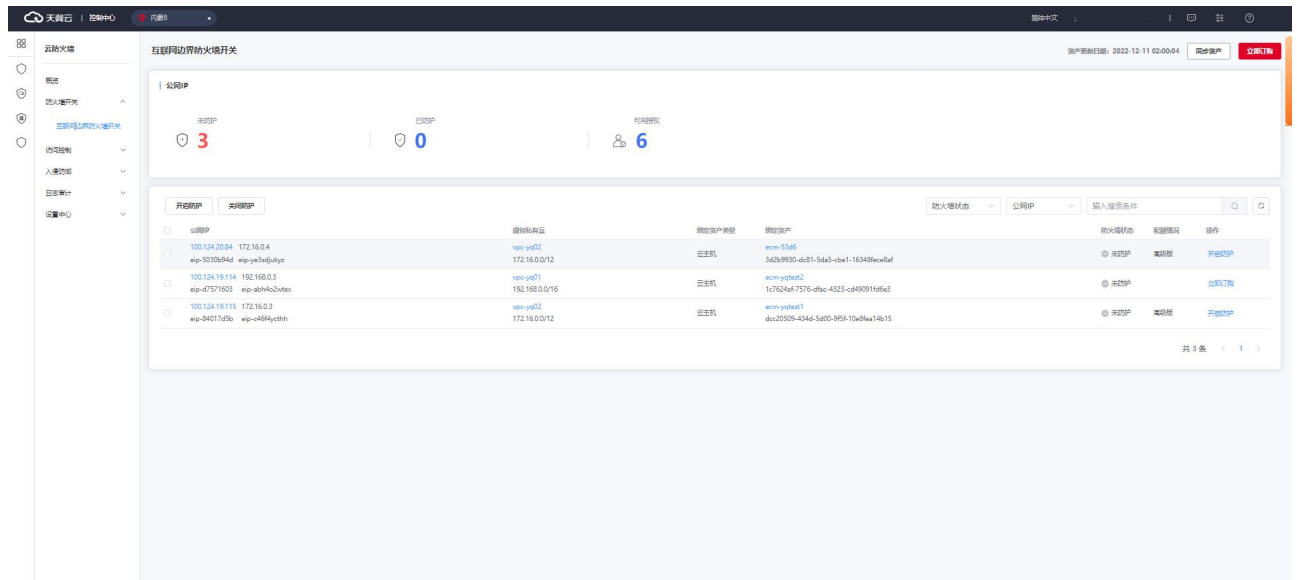


### 3.3. 开启防护

在“配额管理”页面查看使用指引，如下图所示：



单击第 2 步骤中的“开启防护”，跳转至“互联网边界防火墙开关”页面，如下图所示：

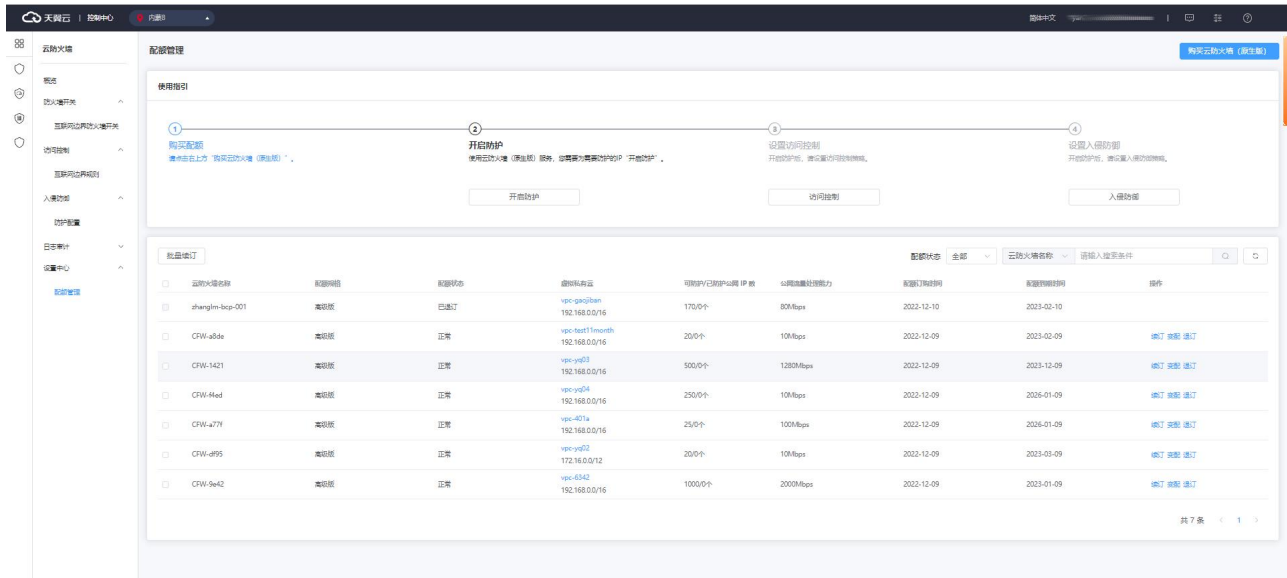


在该页面，可以为您购买过防护配额所在 VPC 中的 IP 开启防护，选中您需要开启防护的 IP，单击操作中的“开启防护”，可为该 IP 开启防护。

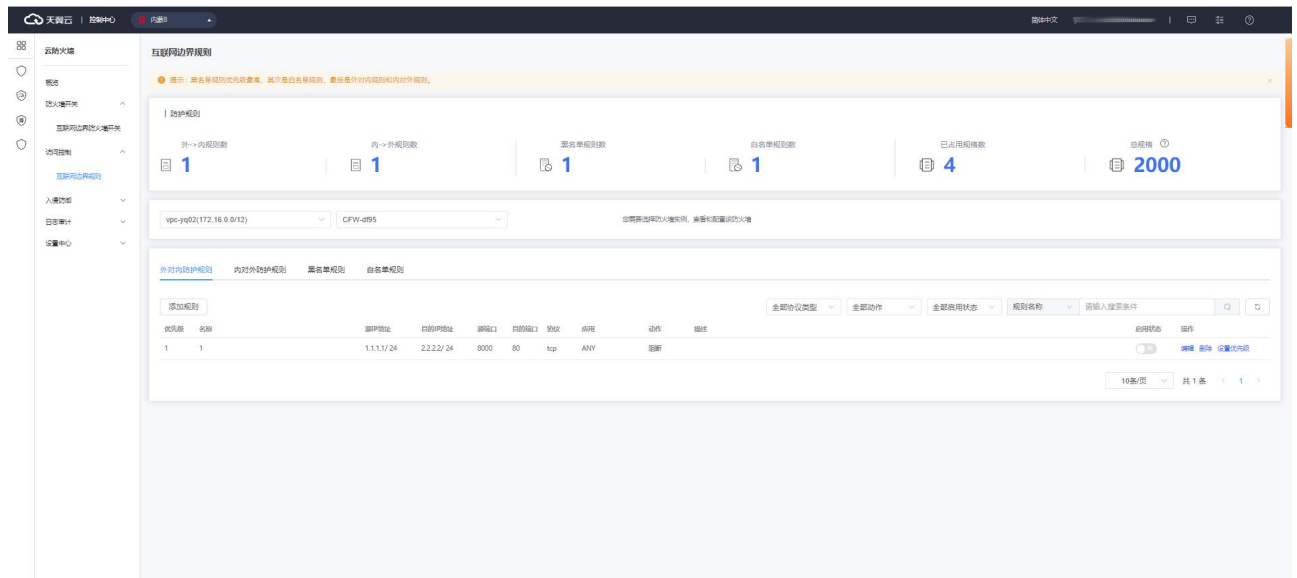


## 3.4. 设置访问控制

在“配额管理”页面查看使用指引，如下图所示：



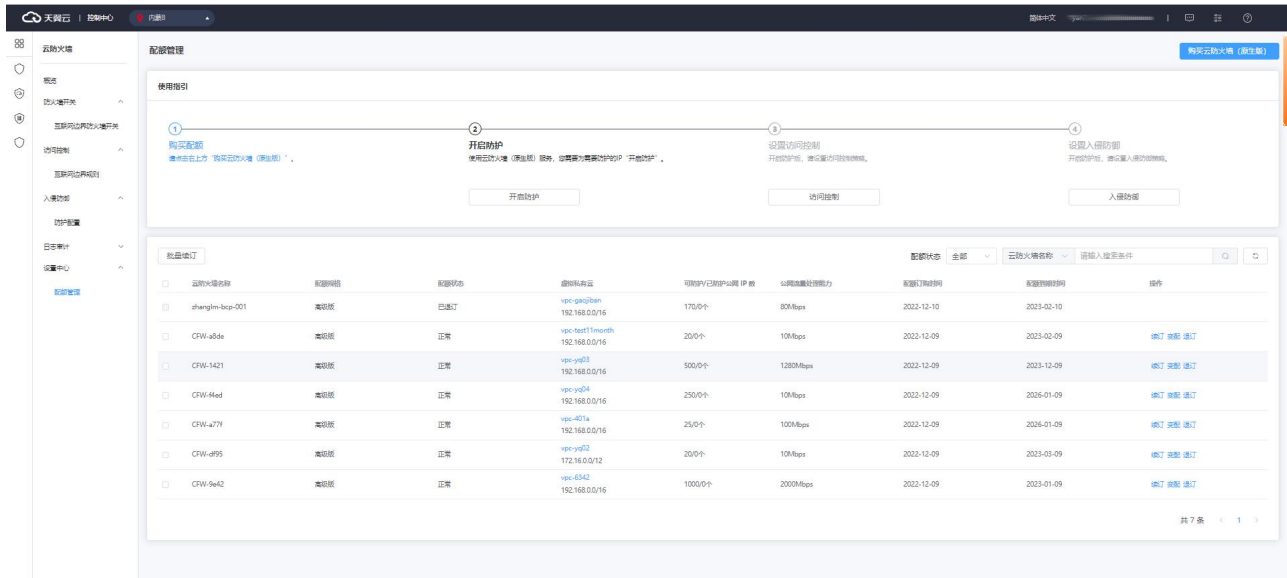
单击第 3 步骤中的“访问控制”，跳转至“互联网边界规则”页面，如下图所示：



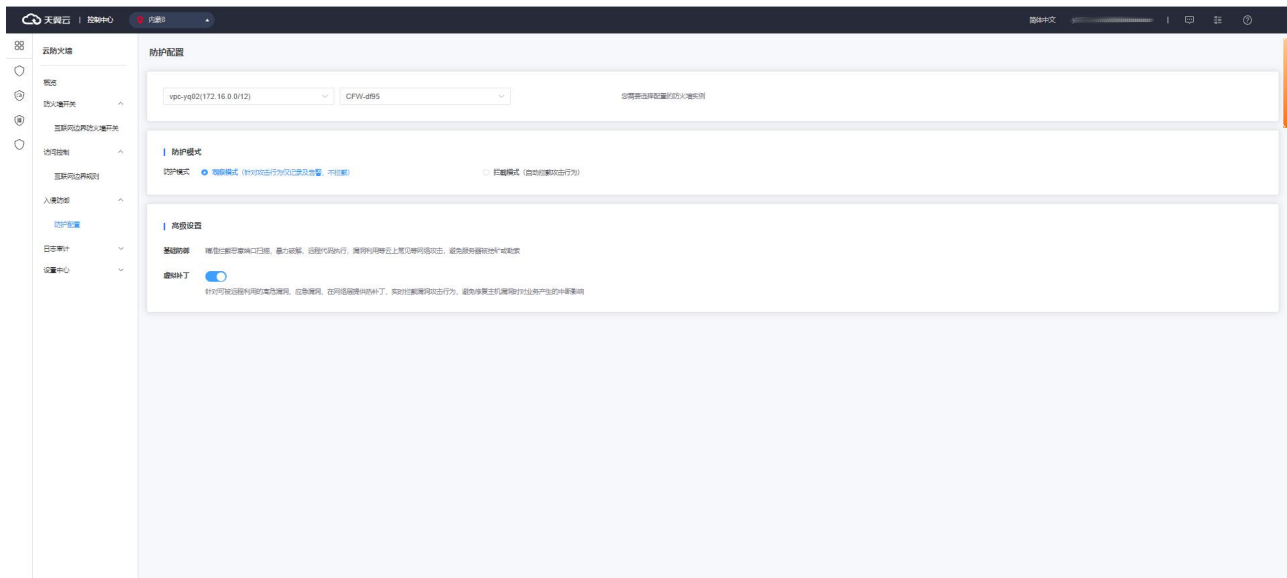
在该页面，添加您需要的访问控制规则，可添加外对内规则数、内对外规则数、黑名单规则数、白名单规则 4 类，可以根据需要分别进行配置。

## 3.5. 设置入侵防御

在“配额管理”页面查看使用指引，如下图所示：



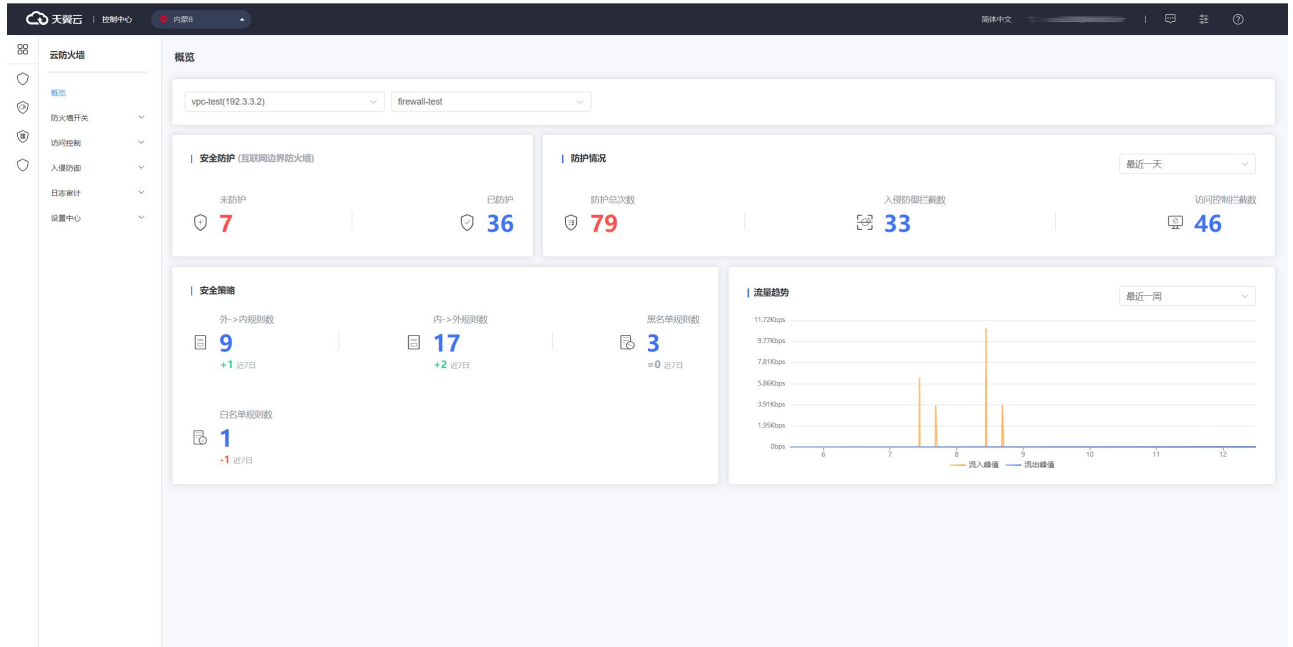
单击第 4 步骤中的“入侵防御”，跳转至“防护配置”页面，如下图所示：



在该页面，配置防护模式，分为观察模式和拦截模式，根据需要进行配置。也可以对虚拟补丁进行开启和关闭。若选择观察模式，则仅针对攻击行为仅记录及告警，不拦截；若选择拦截模式，则自动拦截攻击行为。

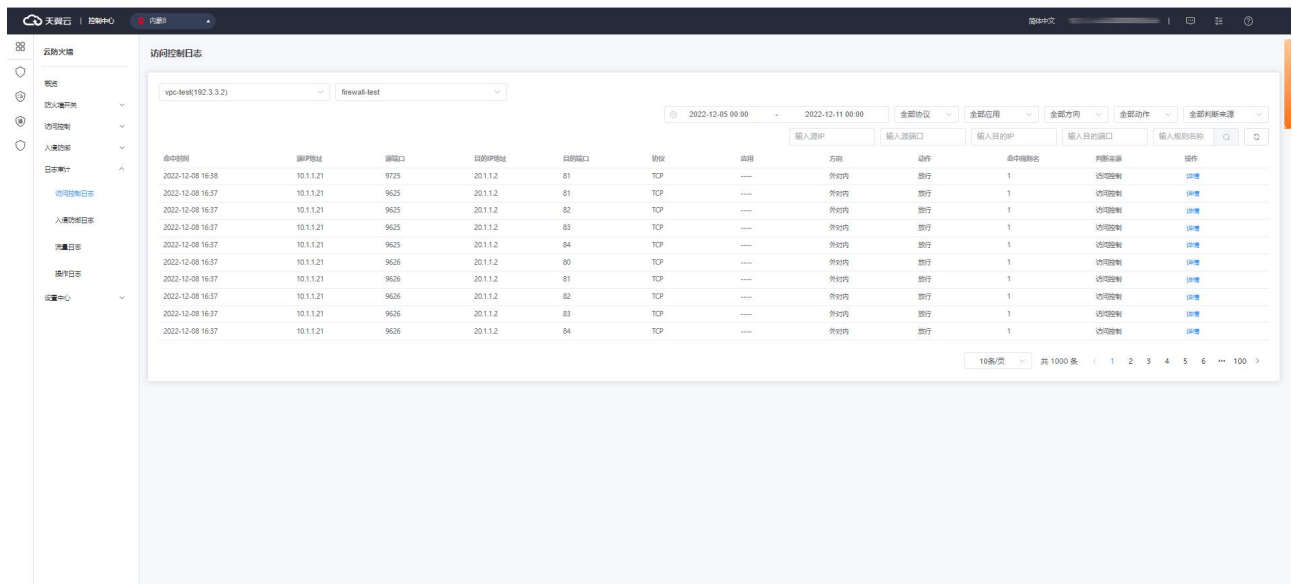
### 3.6. 查看防护结果

选择“概览”，进入概览页面，可查看所在 VPC 的防护概览，包括安全防护、防护情况、安全策略和流量趋势。



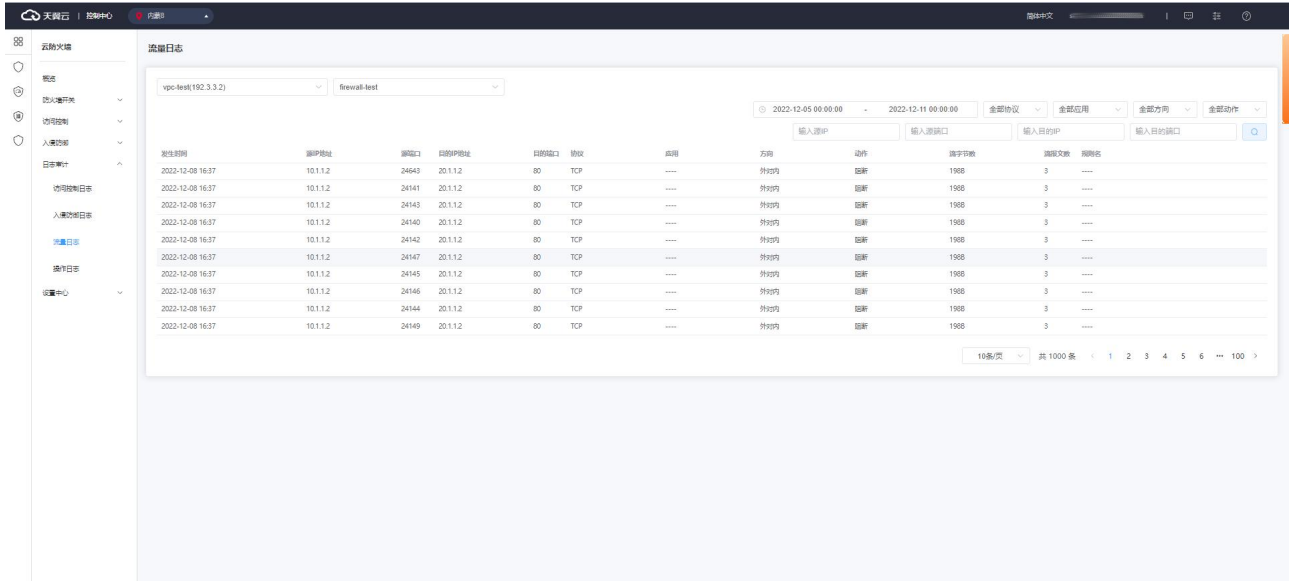
也可以选择“日志审计”，查看访问控制日志、入侵防御日志和流量日志。

访问控制日志如下，展示了可以查看云防火墙基于您在配置的访问控制规则所生成的规则命中记录日志。



命中时间	源IP地址	源端口	目的IP地址	目的端口	协议	方向	动作	命中规则名	判断来源	操作
2022-12-08 16:38	10.1.1.21	9725	20.1.1.2	81	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9625	20.1.1.2	81	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9625	20.1.1.2	82	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9625	20.1.1.2	83	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9625	20.1.1.2	84	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	80	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	81	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	82	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	83	TCP	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	84	TCP	外对内	放行	1	访问控制	详情

入侵防御日志如下，展示了可查看云防火墙基于入侵防御“观察模式”和“拦截模式”所产生的记录的所有安全事件。



流量日志

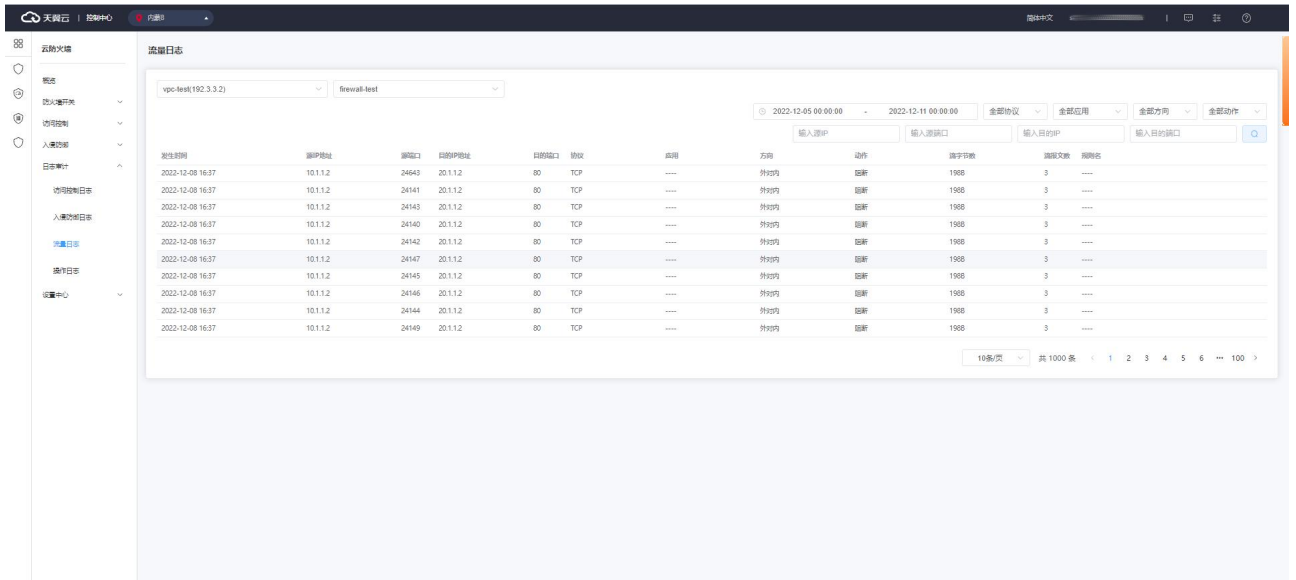
vpc-test(192.3.3.2) firewall-test

2022-12-05 00:00:00 - 2022-12-11 00:00:00

发生时间	源IP地址	源端口	目标IP地址	目标端口	协议	应用	方向	动作	源字节数	目标字节数	规则名
2022-12-08 16:37	10.1.1.2	24643	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24141	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24143	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24140	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24142	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24147	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24145	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24146	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24144	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----
2022-12-08 16:37	10.1.1.2	24149	20.1.1.2	80	TCP	----	外到内	阻断	1988	3	----

10条/页 共 1000 条 < 1 2 3 4 5 6 ... 100 >

流量日志如下，展示了可以查看互联网边界防火墙基于出站和入站所产生的南北向流量信息。



## 3.7. 入门实践

当您完成防火墙的购买和防护开通后，可以根据您的需要进行一系列常用实践，防火墙常用实践如下表。

实践	描述
<a href="#">云防火墙最佳实践</a>	介绍如何选择最适宜用户使用场景和带宽的防火墙规格，以及介绍如何启用防护配置策略，配置防护规则，适用于初次使用防火墙，不知道如何选择适宜自己场景的防火墙规格以及不知道如何启用防火墙产品的用户及场景
<a href="#">配置访问控制策略最佳实践</a>	介绍如何进行访问控制策略配置，在日常生产场景中，常用哪些访问控制策略应该需要配置，适用于安全应用了解较少，需要进行标准化策略防护的用户及场景

## 4.1. 购买

### 4.1.1. 订购

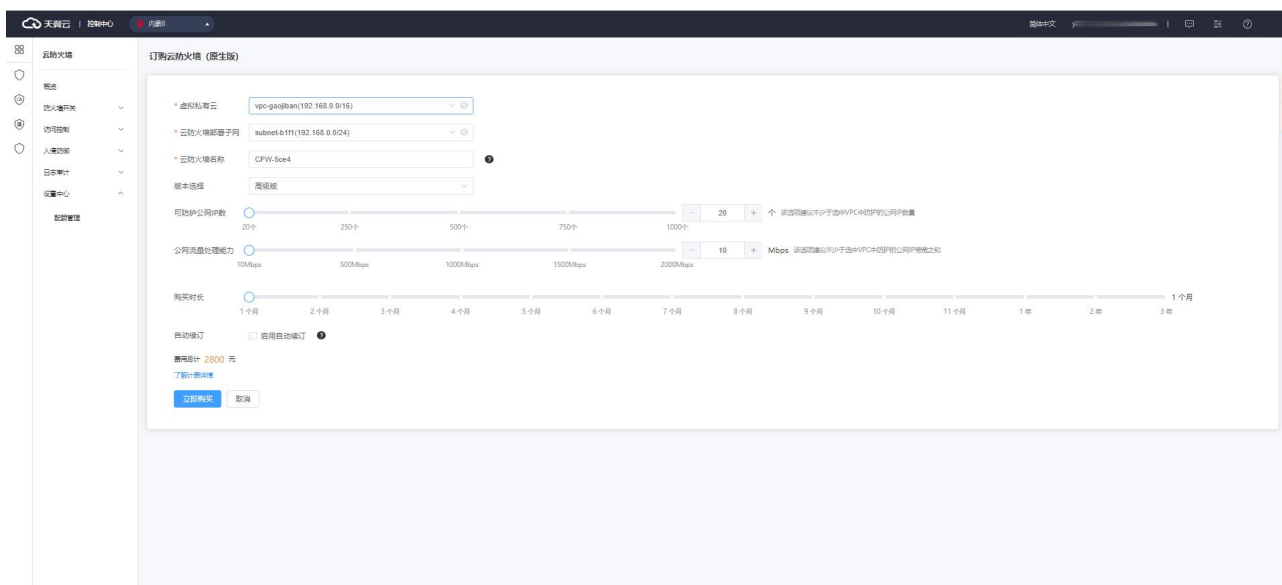
以下为云防火墙（原生版）的购买流程。

当您具备已通过实名认证的 ctyun 账号后，可以通过以下两种方式开通云防火墙（原生版）：

1. 在天翼云官网首页选择“产品->安全->网络安全->云防火墙（原生版）”。进入云防火墙（原生版）产品详情页后，选择“立即开通”，如下图所示：



进入到云防火墙（原生版）产品购买页面，如下图所示：



您需要选择虚拟私有云、云防火墙部署子网、云防火墙名称、版本、可防护公网 IP 数、公网流量处理能力和购买时长和是否自动续订。

虚拟私有云：该下拉选项中展示您在该地域的所有 VPC，选择您需要防护的 VPC。由于一个 VPC 只能购买一个 VPC 配额，因此已经购买配额的 VPC 不能重复进行购买。

云防火墙部署子网：可以下拉选择用户该 VPC 中的子网，展示该子网 ID 和子网网段。需要您在需要防护的 VPC 中创建一个子网掩码不大于 28 的子网网段，在此处进行选择，用于云防火墙的部署，并确保该子网中不进行任何业务配置，只用于云防火墙的部署。

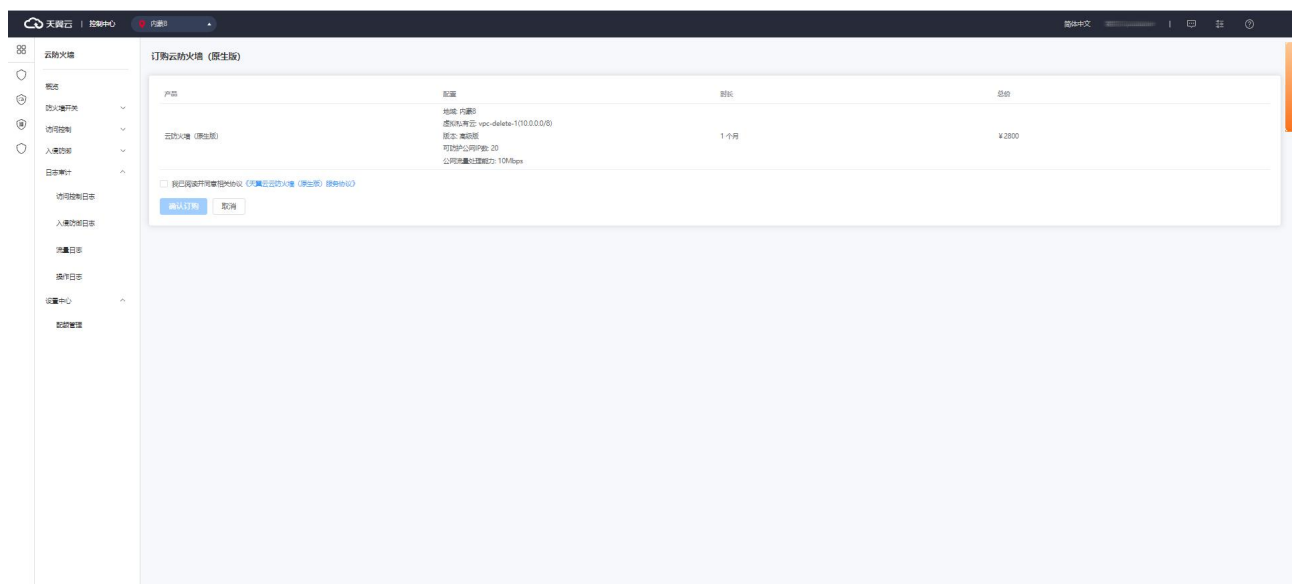
云防火墙名称：只能由数字、字母、-组成，不能以数字和-开头、以-结尾，且长度为 2-63 字符。

可防护公网 IP 数：可以单击加减号调整防护公网 IP 数，步长为 1，也可以在其中直接输入。可防护公网 IP 数的范围是 20 个-1000 个。

公网流量处理能力：可以单击加减号调整公网流量处理能力，步长为 5，也可以在其中直接输入。公网流量处理能力 10Mbps-2000Mbps。

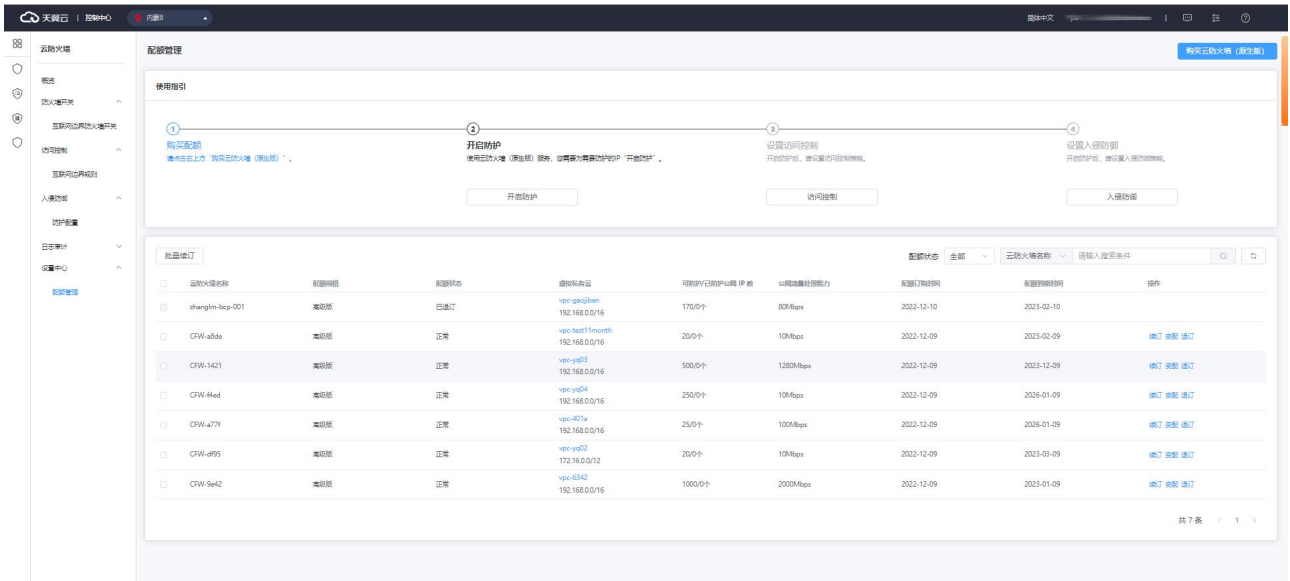
自动续订：按月购买自动续订周期为 3 个月，按年购买自动续订周期为 1 年。您可以在续订管理中修改自动续订周期。

以上参数均选择完毕后，勾选我已阅读并同意相关协议《天翼云云防火墙（原生版）协议》，点击“立即购买”按钮，进入如下页面：



您需要确认地域、虚拟私有云、版本、可防护公网 IP 数、公网流量处理能力、购买时长和总价，确认后单击“确认订购”后即可完成订购。若未确认则单击“上一步”返回订购页面重新选择。

订购成功后即可在“配额管理”页面查看已购买的高级版配额，如下图所示：



2. 在天翼云官网首页选择“控制中心”，如下图所示：

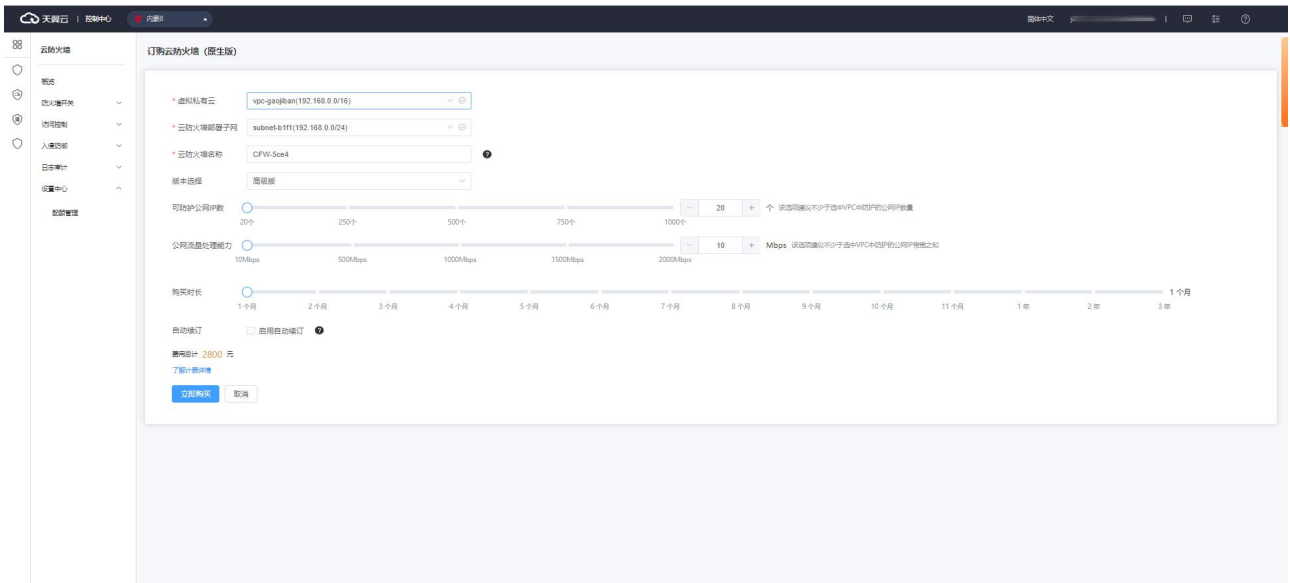


在天翼云控制台中，安全分类下，点击“云防火墙（原生版）”，





进入云防火墙（原生版）产品购买页面，如下图所示：



您需要选择虚拟私有云、云防火墙部署子网、云防火墙名称、版本、可防护公网 IP 数、公网流量处理能力和购买时长和是否自动续订。

虚拟私有云：该下拉选项中展示您在该地域的所有 VPC，选择您需要防护的 VPC。由于一个 VPC 只能购买一个 VPC 配额，因此已经购买配额的 VPC 不能重复进行购买。

云防火墙部署子网：可以下拉选择用户该 VPC 中的子网，展示该子网 ID 和子网网段。需要您在需要防护的 VPC 中创建一个子网掩码不大于 28 的子网网段，在此处进行选择，用于云防火墙的部署，并确保该子网中不进行任何业务配置，只用于云防火墙的部署。

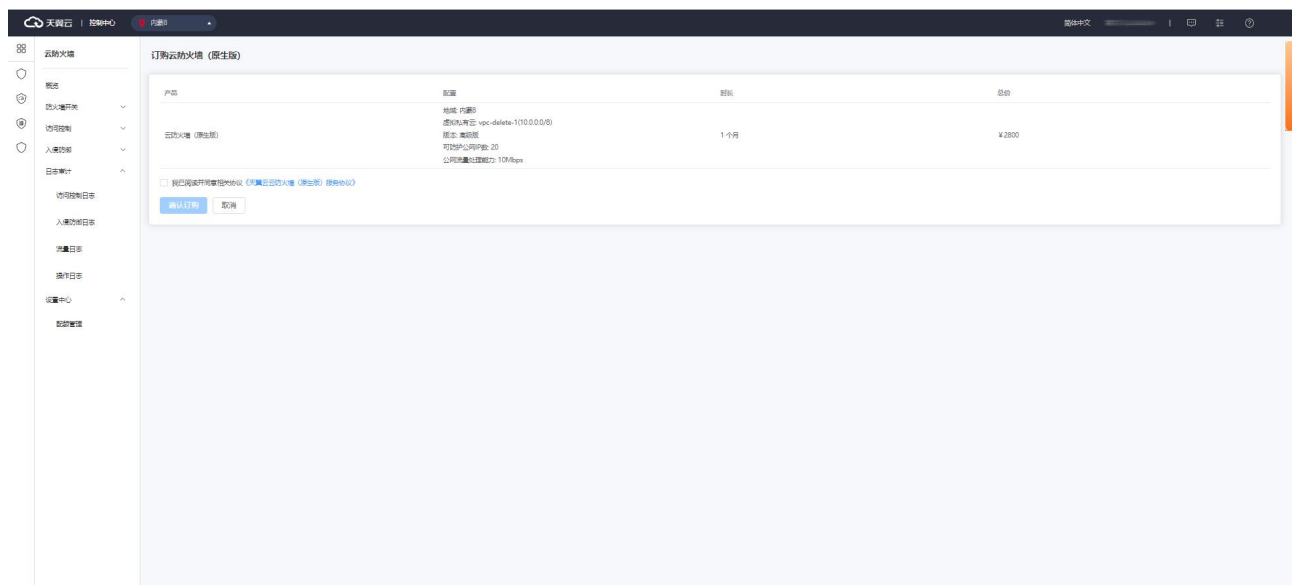
云防火墙名称：只能由数字、字母、-组成, 不能以数字和-开头、以-结尾, 且长度为 2-63 字符。

可防护公网 IP 数：可以单击加减号调整防护公网 IP 数，步长为 1，也可以在其中直接输入。可防护公网 IP 数的范围是 20 个-1000 个。

公网流量处理能力：可以单击加减号调整公网流量处理能力，步长为 5，也可以在其中直接输入。公网流量处理能力 10Mbps-2000Mbps。

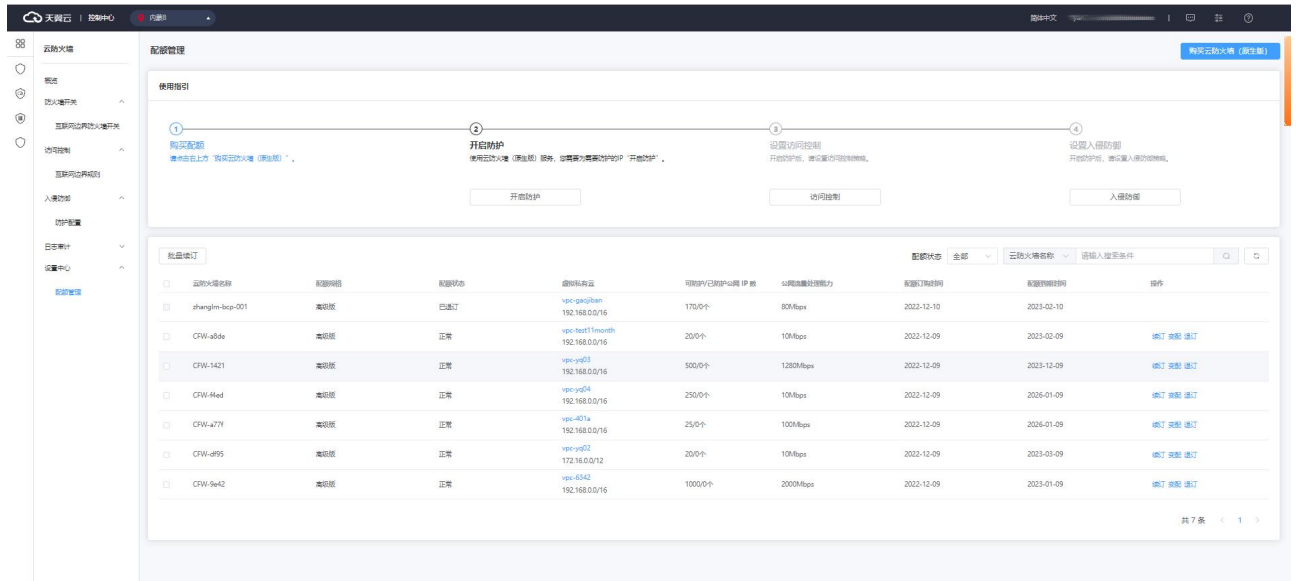
自动续订：按月购买自动续订周期为 3 个月，按年购买自动续订周期为 1 年。您可以在续订管理中修改自动续订周期。

以上参数均选择完毕后，勾选我已阅读并同意相关协议《天翼云云防火墙（原生版）协议》，点击“立即购买”按钮，进入如下页面：



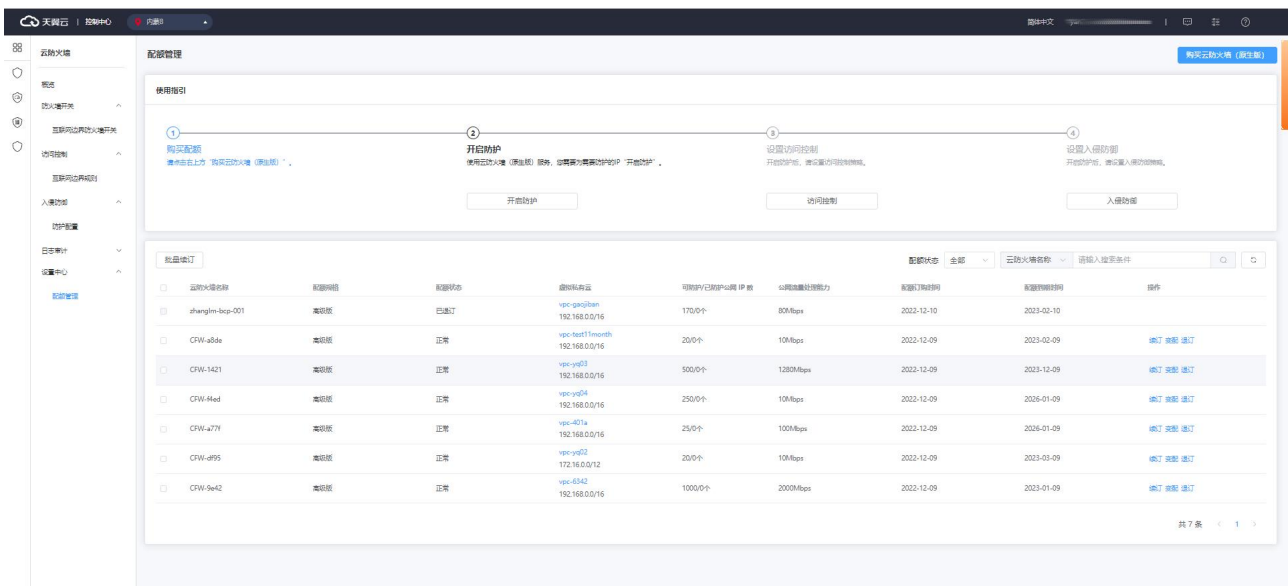
您需要确认地域、虚拟私有云、版本、可防护公网 IP 数、公网流量处理能力、购买时长和总价，确认后单击“确认订购”后即可完成订购。若未确认则单击“上一步”返回订购页面重新选择。

订购成功后即可在“配额管理”页面查看已购买的高级版配额，如下图所示：

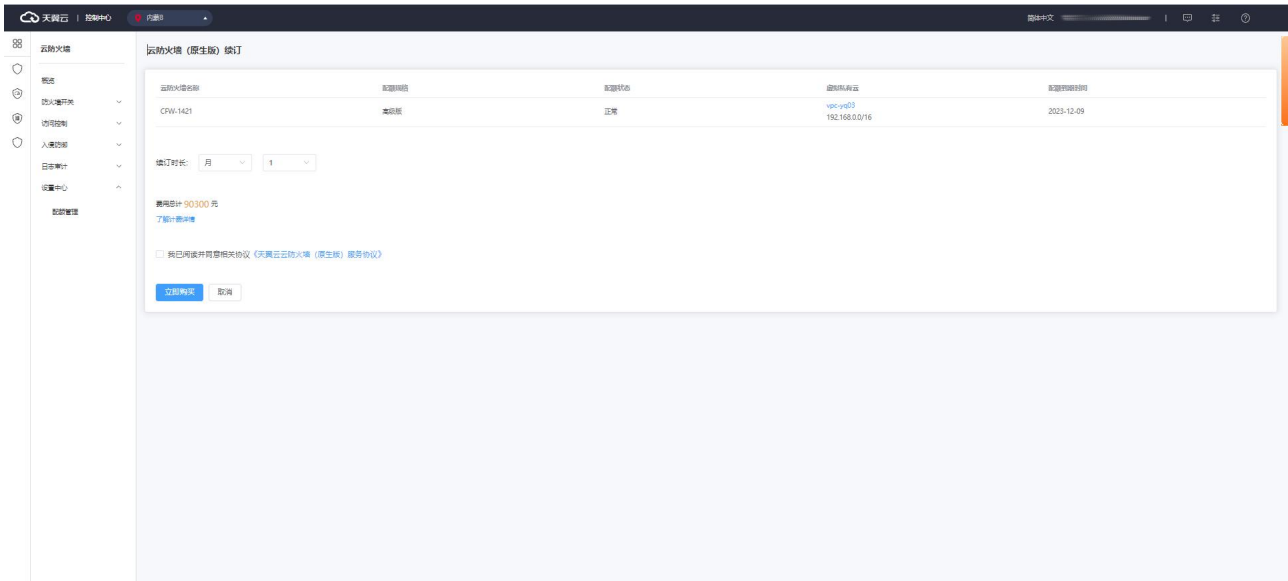


## 4.1.2. 手动续订

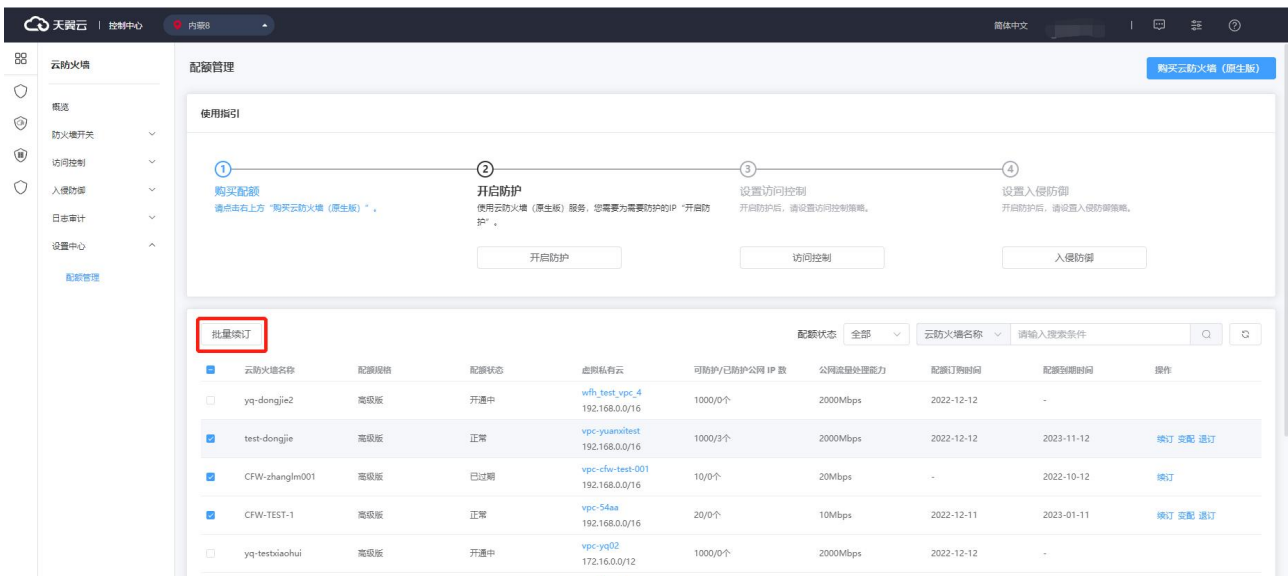
在“设置中心->配额管理”中查看您已经订购的配额，配额状态为“正常”和“已到期”的高级版配额才可以续订。选择所需续订的配额，点击“续订”，如下图所示：



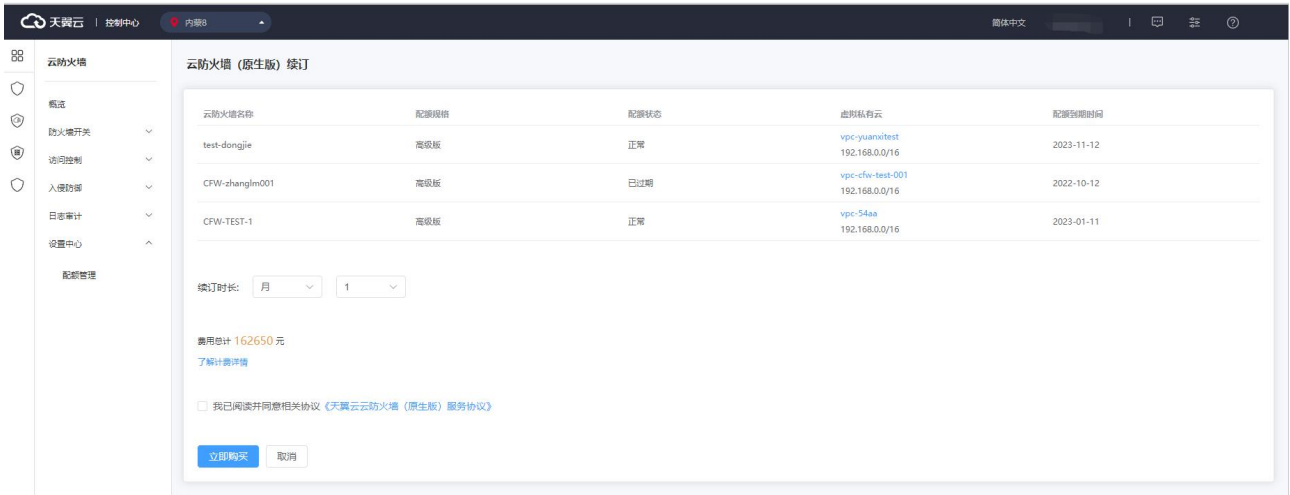
在下图续订页面中，选择续订时长，勾选我已阅读并同意相关协议《天翼云云防火墙（原生版）协议》后，并点击“立即购买”后即可进行续订。当续订周期达到1年或以上时，续订单将可享受包年折扣，续订金额显示折后价。



您也可以对多个配额进行批量续订。在“设置中心->配额管理”中查看您已经订购的配额，选择所需续订的配额，点击“批量续订”，如下图所示：



在下图续订页面中，选择续订时长，勾选我已阅读并同意相关协议《天翼云云防火墙（原生版）协议》后，并点击“立即购买”后即可进行续订。当续订周期达到1年或以上时，续订单将可享受包年折扣，续订金额显示折后价。



### 4.1.3. 自动续订

#### 开通自动续订

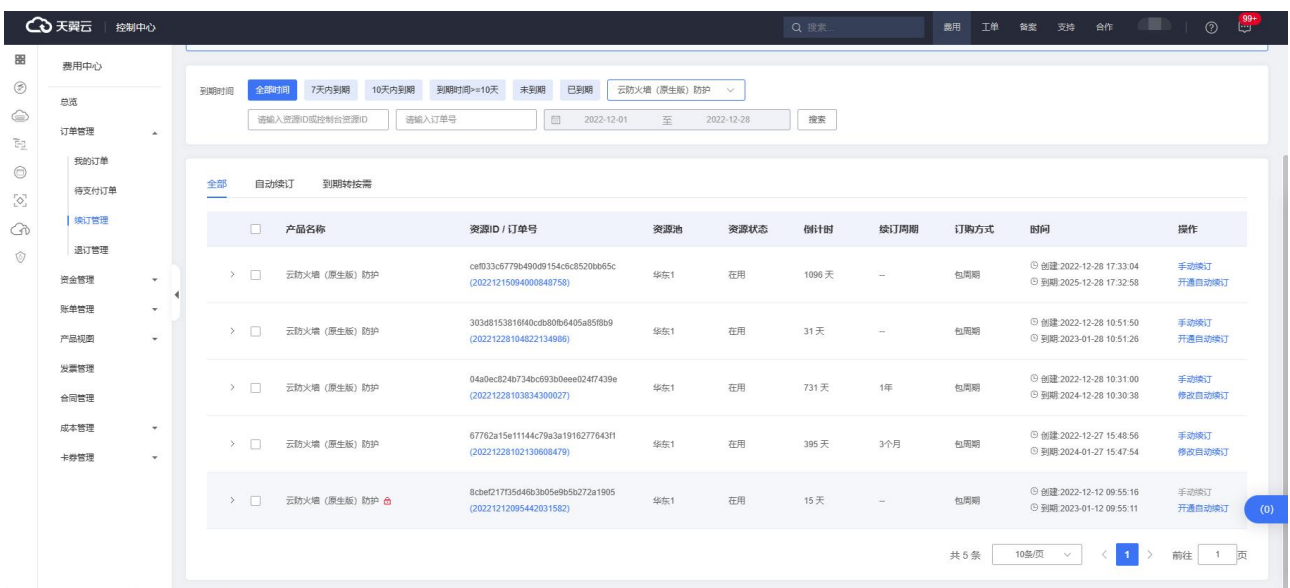
步骤 1 进入“续订管理”页面。

步骤 2 设置查询条件。

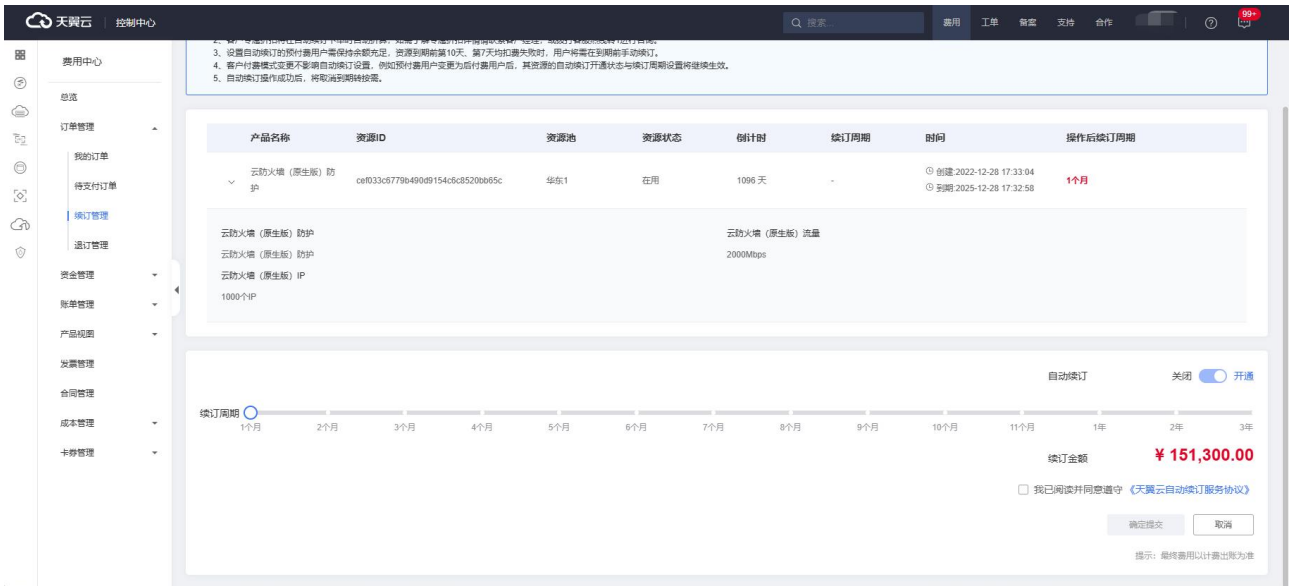
可综合利用到期时间、产品类型、是否开通自动续订查询资源。

由于自动续订两次下单时间为到期前 10 天和前 7 天，建议您选择“到期时间 $\geq$ 10 天”，“未开通自动续订”的云防火墙（原生版）。

步骤 3 在资源页面找到待续订的资源，单击操作列的“开通自动续订”，如下图所示：



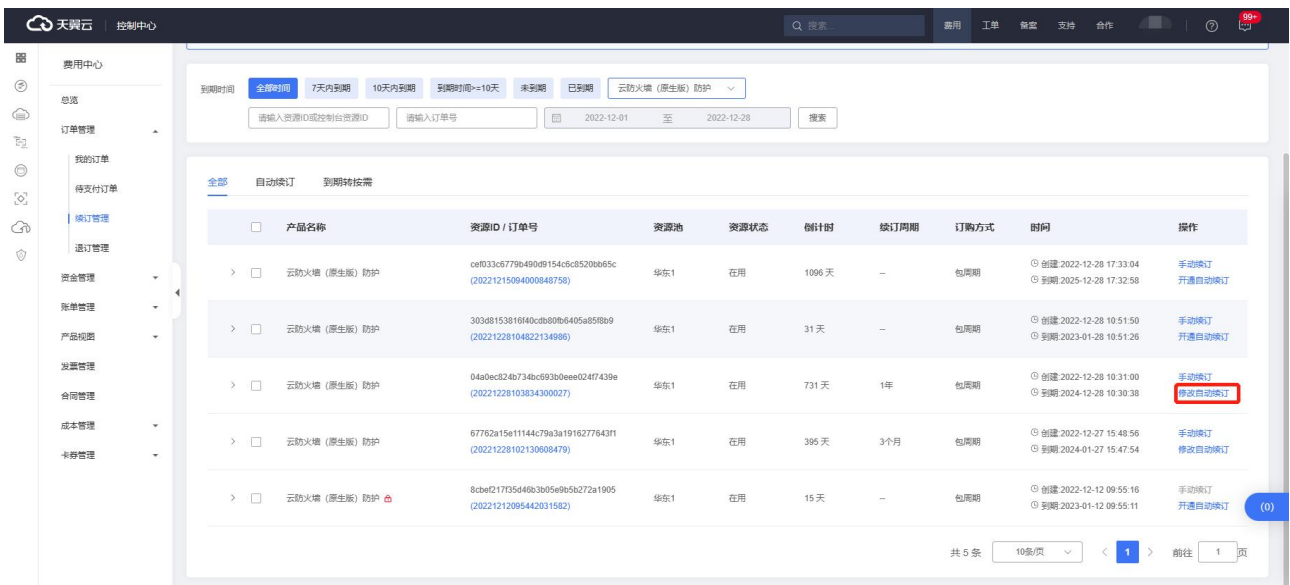
步骤 4 设置“自动续订周期”，仔细阅读《天翼云自动续订服务协议》，如果同意全部约定，则勾选“我已阅读并同意遵守《天翼云自动续订服务协议》的约定”，单击“确定提交”，如下图所示：



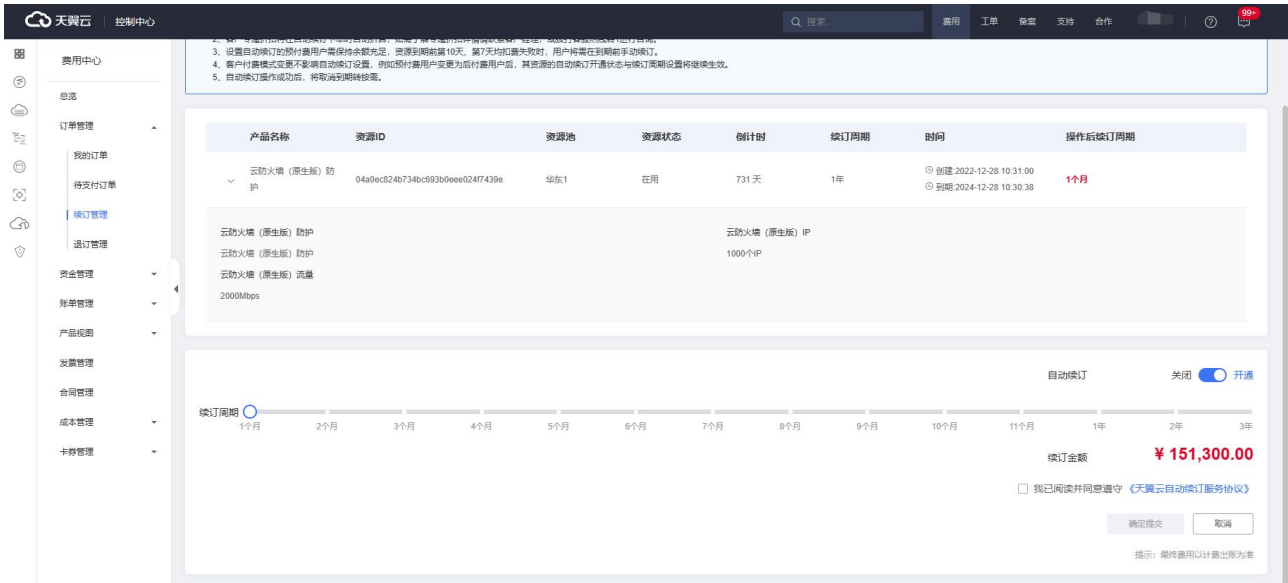
## 修改自动续订周期

步骤 1 进入“续订管理”页面。

步骤 2 在资源页面找到待修改自动续订的资源，单击操作列的“修改自动续订”。



步骤 3 拖动“续订周期”可修改自动续订周期。

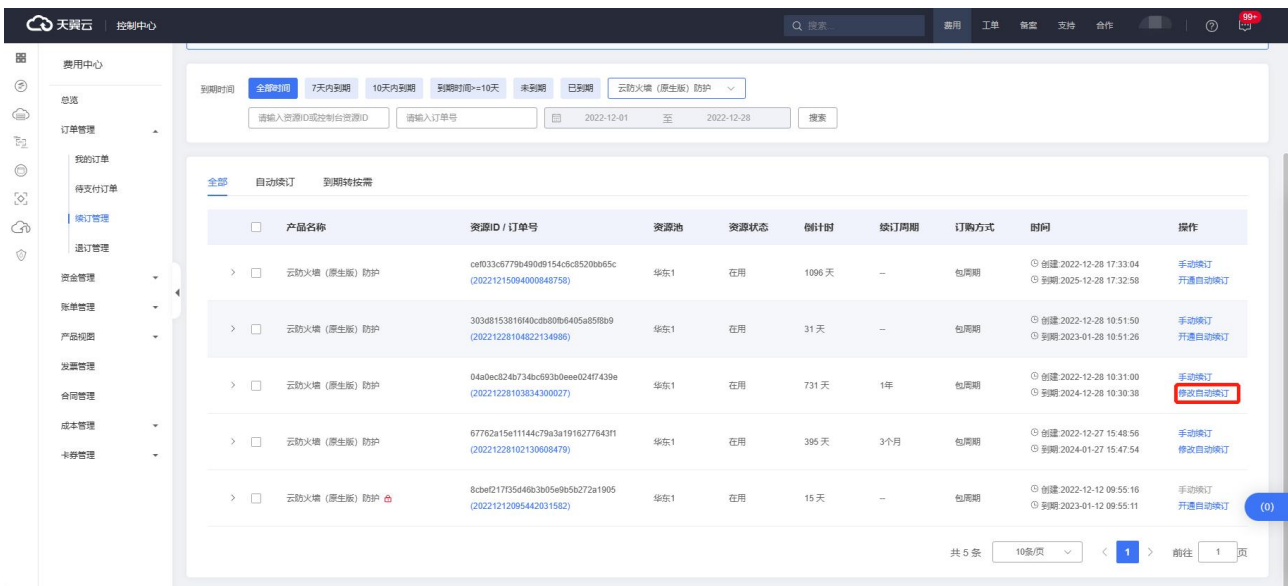


步骤 4 勾选“我已阅读并同意遵守《天翼云自动续订服务协议》的约定”，点击“确定提交”。

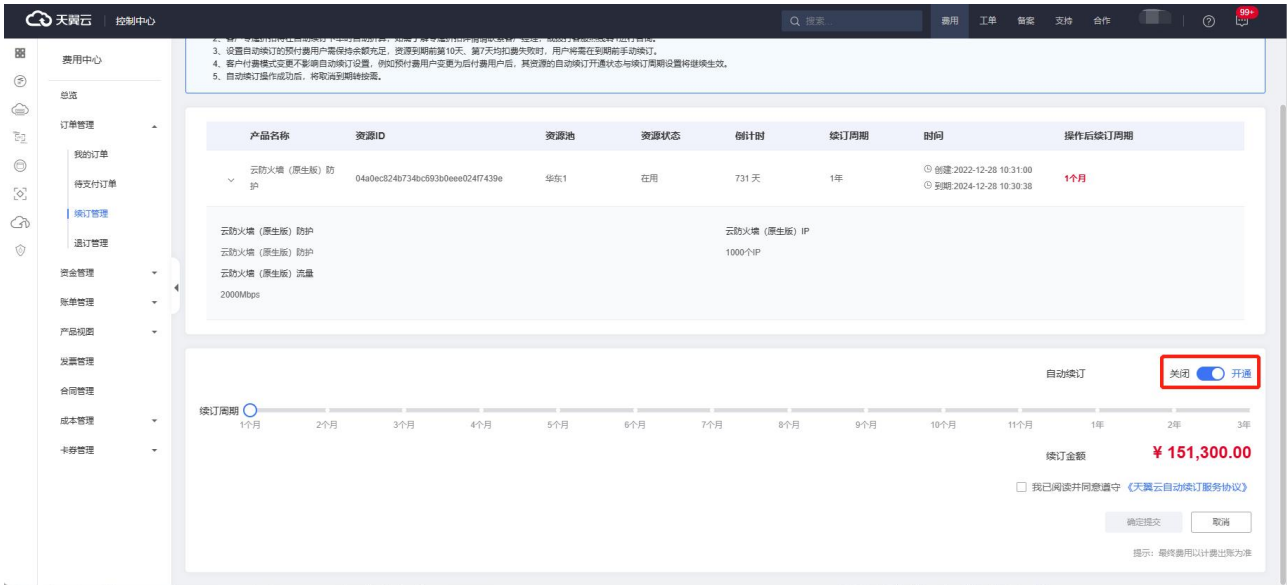
## 关闭自动续订

步骤 1 进入“续订管理”页面。

步骤 2 在资源页面找到待修改自动续订的资源，单击操作列的“修改自动续订”。

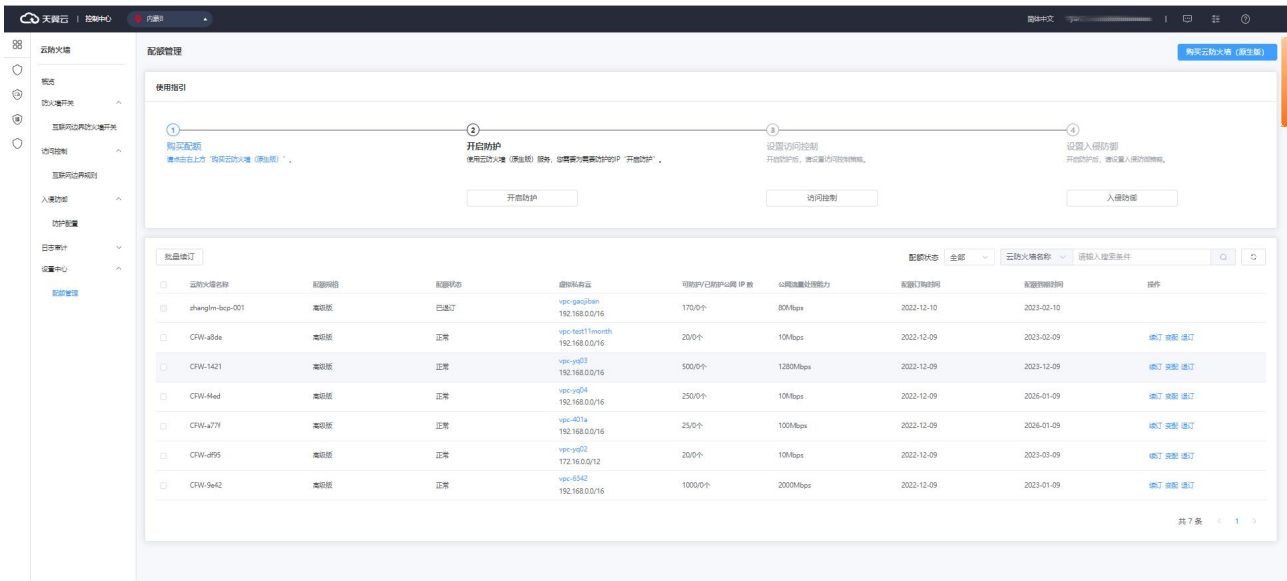


步骤 3 点击“自动续订”后方的关闭/开通按钮，单击“确定提交”。



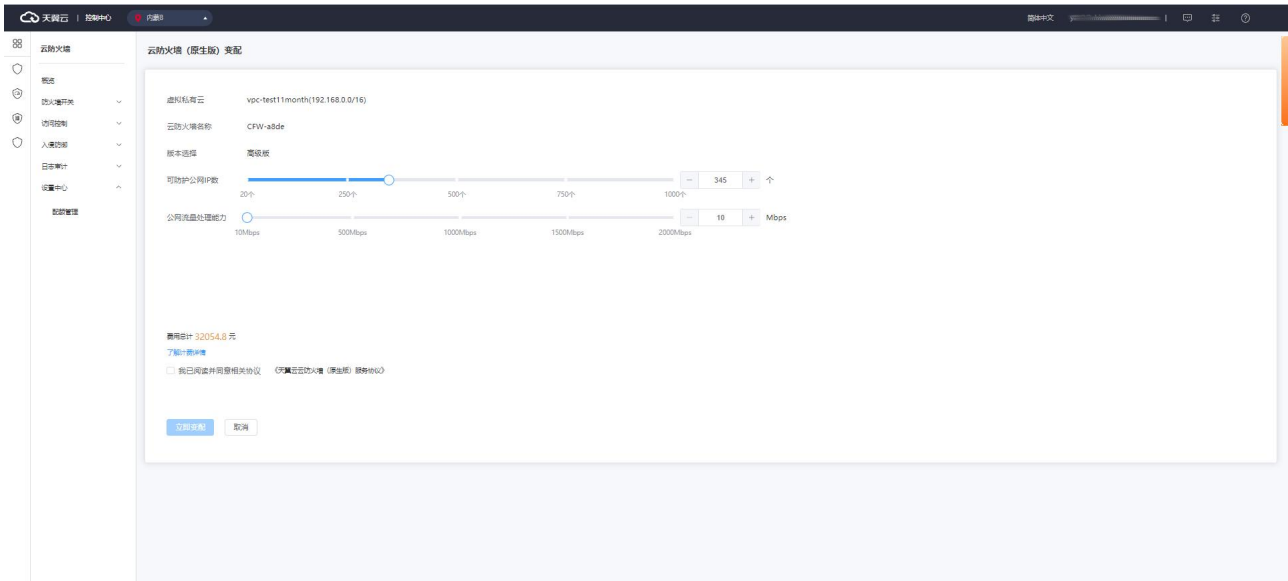
### 4.1.4. 变配

在“设置中心->配额管理”中查看您已经订购的配额，配额状态为“正常”的高级版配额才可以变配。选择所需变配的配额，点击“变配”，如下图所示：



您可以对选定配额的公网 IP 数、公网流量处理能力数值进行调整，如下图所示：





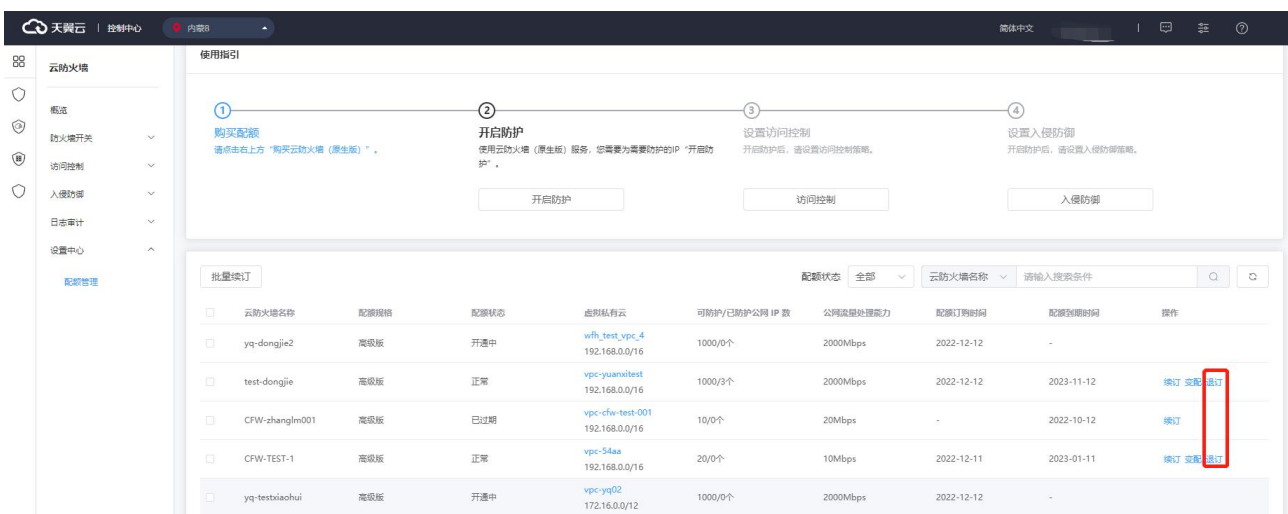
可防护公网 IP 数：可以单击加减号调整防护公网 IP 数，步长为 1，也可以在其中直接输入。可防护公网 IP 数的范围是 20 个-1000 个。

公网流量处理能力：可以单击加减号调整公网流量处理能力，步长为 5，也可以在其中直接输入。公网流量处理能力 10Mbps-2000Mbps。

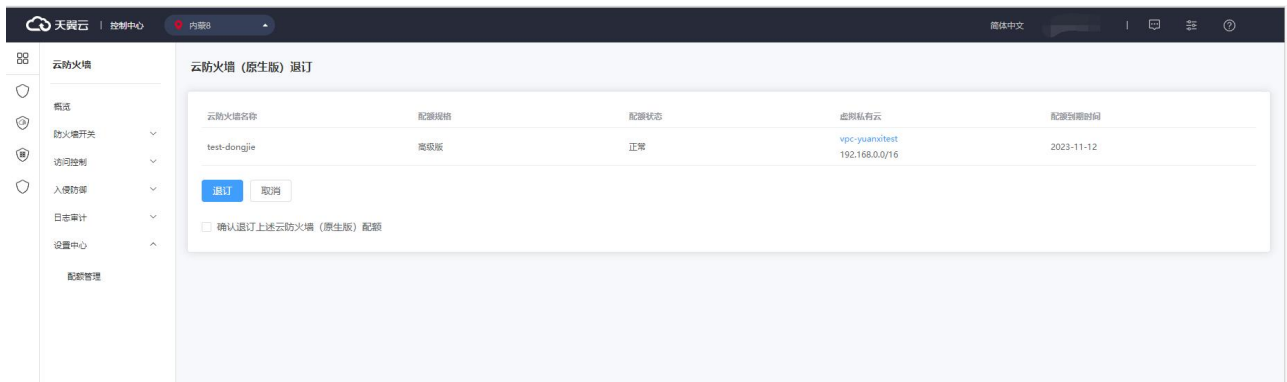
当您进行降配时，降配后的 IP 规格不能小于该 VPC 内正在防护的公网 IP 数，且需要分步降配可防护公网 IP 数和公网流量处理能力。

## 4.1.5. 退订

在“设置中心->配额管理”中查看您已经订购的配额，选择所需退订的配额，点击“退订”，如下图所示：

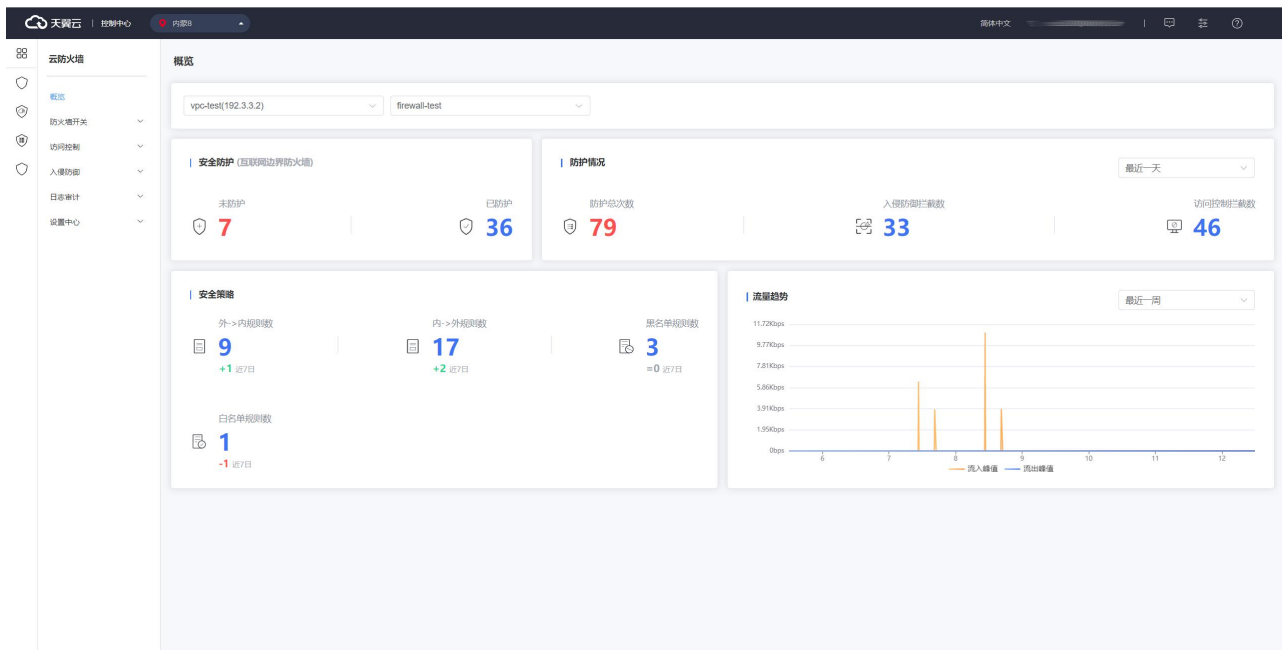


在下图退订页面中，选择退订原因，勾选我已确认本次退订金额和相关费用后，并点击“退订”后即可进行退订。



## 4.2. 概览

概览主要分为安全防护、安全策略、防护情况、流量趋势四大统计功能，如下图所示。



安全防护：展示互联网边界防火墙的防护总体情况。

安全策略：展示客户配置的访问控制策略的情况。

防护情况：展示了防护的总体情况。

流量趋势：展示了近期已开启防护的资产上的互联网边界防火墙。

### 4.2.1. 安全防护



如上图所示，安全防护展示了互联网边界防火墙的防护总体情况，包括已开启和未开启防护的 IP，对应“互联网边界防火墙开关”页面上的统计。

未防护：展示未开启防护的 IP 数量，点击数字时会跳转至“防火墙开关-互联网边界防火墙开关”界面。

已防护：展示已开启防护的 IP 数量，点击数字时会跳转至“防火墙开关-互联网边界防火墙开关”界面。

## 4.2.2. 安全策略



如上图所示，安全策略展示了客户配置的访问控制策略的情况，分别为外->内规则数、内->外规则数、黑名单规则数、白名单规则数，对应访问控制页面上的统计。

外->内规则数：展示外对内防护规则数量，点击数字时会跳转至“访问控制-互联网边界规则”页面。

内->外规则数：展示内对外防护规则数量，点击数字时会跳转至“访问控制-互联网边界规则”页面。

黑名单规则数：展示添加的黑名单规则数量，点击数字时会跳转至“访问控制-互联网边界规则”页面。

白名单规则数：展示添加的白名单规则数量，点击数字时会跳转至“访问控制-互联网边界规则”页面。

## 4.2.3. 防护情况



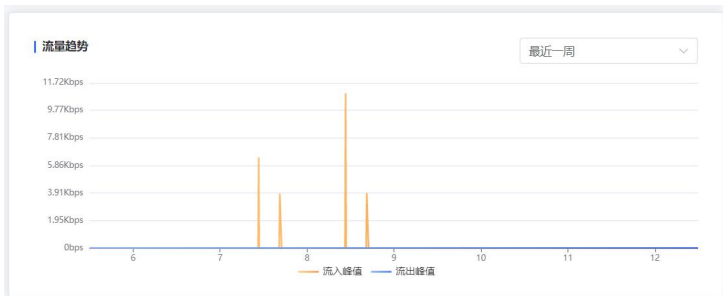
如上图所示，防护情况展示了防护的总体情况，包括入侵防御拦截数和访问控制拦截数，防护总次数为 2 项之和。统计维度分为最近一天和最近一周。

防护总次数：展示了近期云防火墙（原生版）为您的资产触发的安全防护的总次数，等于入侵防御拦截数与访问控制拦截数的总和。

入侵防御拦截数：展示了入侵防御拦截的数量。

访问控制拦截数：展示了访问控制拦截的数量。

#### 4.2.4. 流量趋势

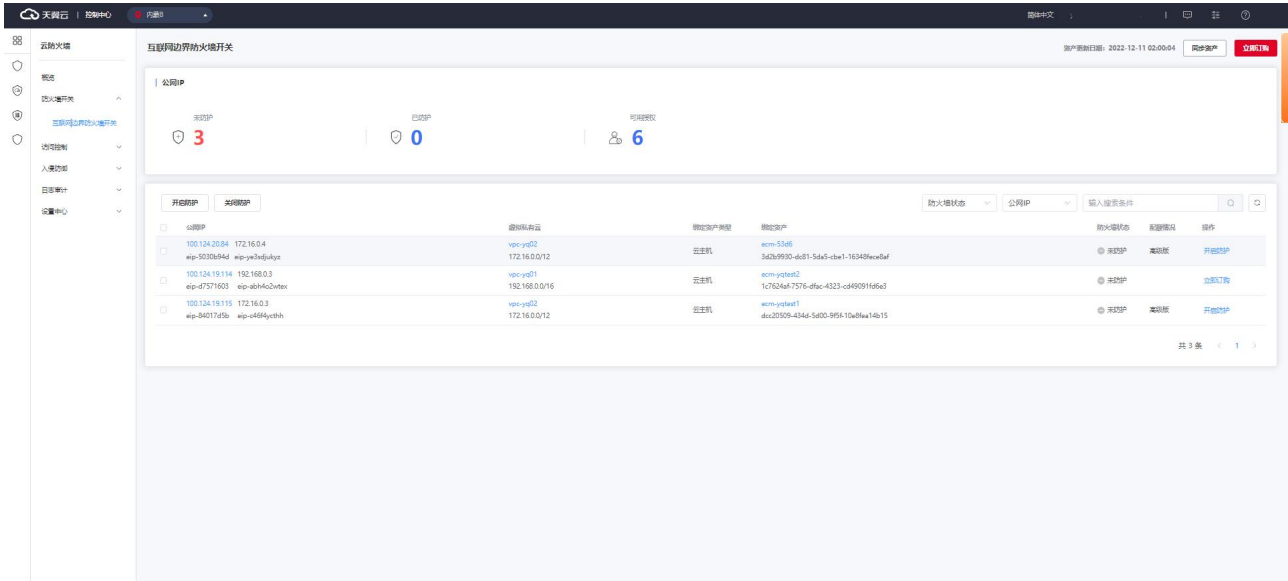


如上图所示，展示了近期已开启防护的资产上的互联网边界防火墙。

时间范围：可选择最近一天和最近一周。入方向流量趋势和出方向流量趋势分别为您展示了该 VPC 内所有防护 IP 的入流量之和出流量之和的流量趋势。

## 4.3. 防火墙开关

防火墙开关分为同步资产、防护情况统计和防护 IP 列表部分 3 大模块，如下图所示。

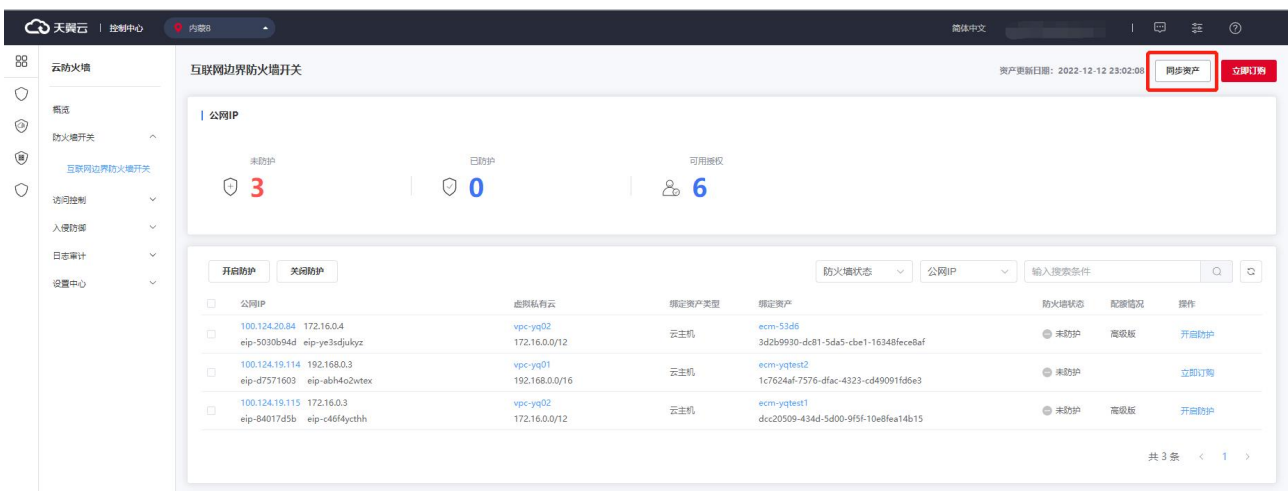


### 4.3.1. 同步资产

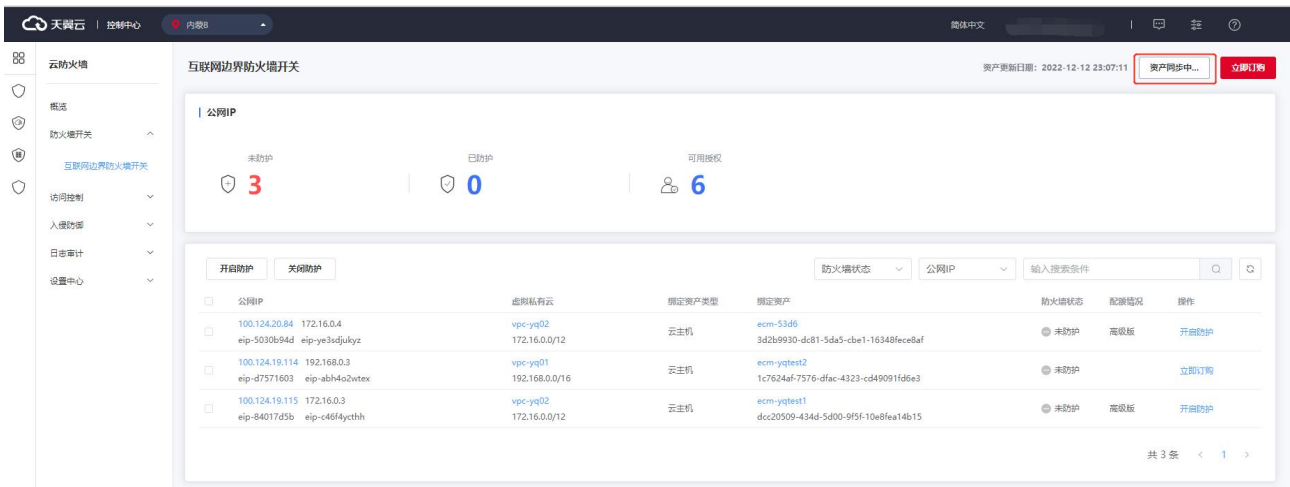
同步资产分为自动同步和手动同步两种方式。

自动同步：每 24 小时同步一次，每天会自动为您进行同步。

手动同步：单击“同步资产”，会同步该您的所有资产，如下图所示：



在资产同步过程中，会显示资产同步中...，如下图所示：



每次资产更新后，无论是自动同步或是手动同步资产更新时间均会更新为最新的同步完成时间。

您首次购买后进入，到达“配额管理”页面，同时自动为您同步资产，同步完成后，公网 IP 默认处于关闭防护状态，需要您自己“开启防护”，并去配置相关的规则。

### 4.3.2. 防护情况统计



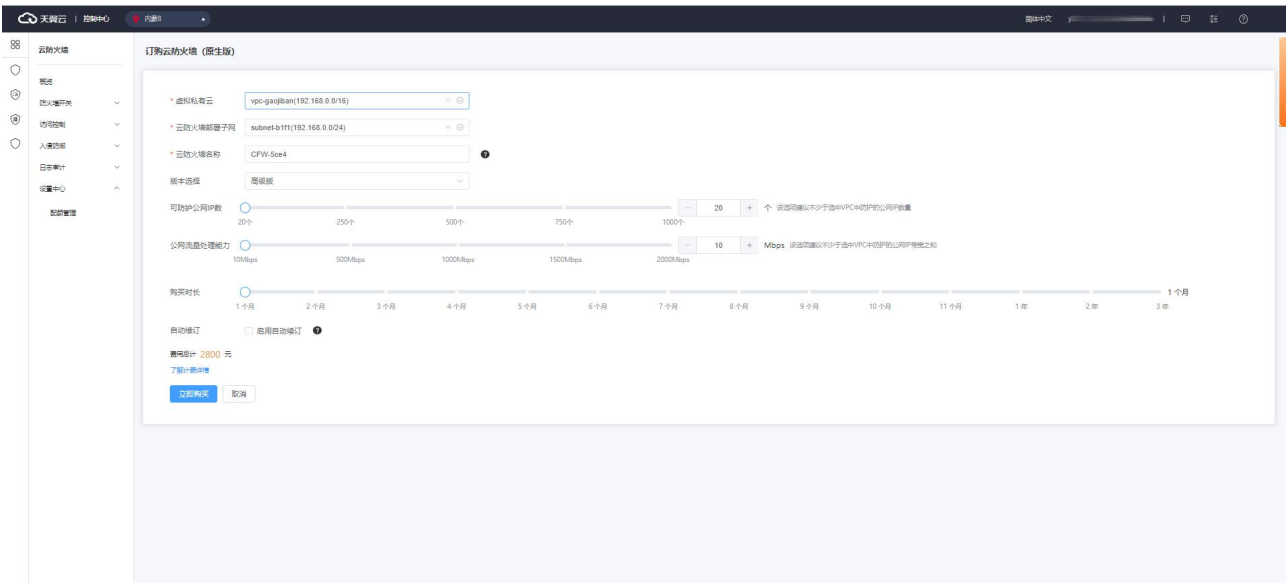
如上图所示，公网 IP 统计了您已开启和未开启防护的公网 IP，对应防火墙状态中的“已防护”和“未防护”状态，未防护的统计所有绑定资产类型对应的公网 IP。可用授权展示已经购买的云防火墙配额数，每个配额可防护一个 VPC，您可以为该 VPC 中的所有 IP 开启防护。

### 4.3.3. 防护 IP 列表

公网IP	虚拟私有云	绑定资产类型	绑定资产	防火墙状态	配额情况	操作
100.124.20.84 eip-5030b94d eip-ye3sdjulyz	vpc-yq02 172.16.0.0/12	云主机	ecm-53d6 3d2b9930-dc81-5da5-cbe1-16348fccc8af	未防护	高级版	开启防护
100.124.19.114 eip-d7571603 eip-abh4a2vtex	vpc-yq01 192.168.0.0/16	云主机	ecm-yqtest2 1c7624af-7576-dfac-4323-cd49091fd6e3	未防护		立即订购
100.124.19.115 eip-84017d5b eip-c46f4ythh	vpc-yq02 172.16.0.0/12	云主机	ecm-yqtest1 dccc20509-434d-5d00-9f5f-10e8fea14b15	未防护	高级版	开启防护

如上图所示，防护 IP 列表展示您所有 VPC 内的绑定云主机资产的公网 IP。列表包括公网 IP（实例名称、ID）、虚拟私有云（VPC 名称、VPC 网段）、绑定资产类型、绑定资产（资产名称、ID）、防火墙状态、配额情况和操作。实例 ID 和名称分别为该公网 IP 的 ID 和名称。

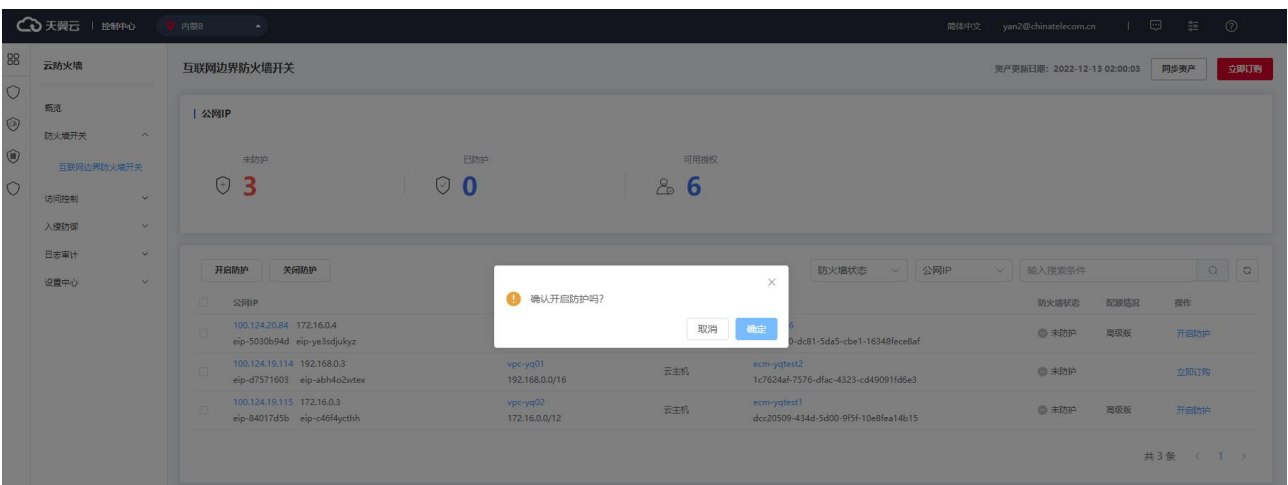
选择一个 VPC 后，需要一个防火墙配额去防护；但是针对与 VPC 中的每个 ip，需要单独去开启和关闭防护。已绑定云主机资产的 EIP，且未购买防火墙时，可选择“立即订购”，单击后跳转至订购页面，如下图所示。



防护 IP 列表可根据防火墙状态、公网 IP 和虚拟私有云进行筛选。

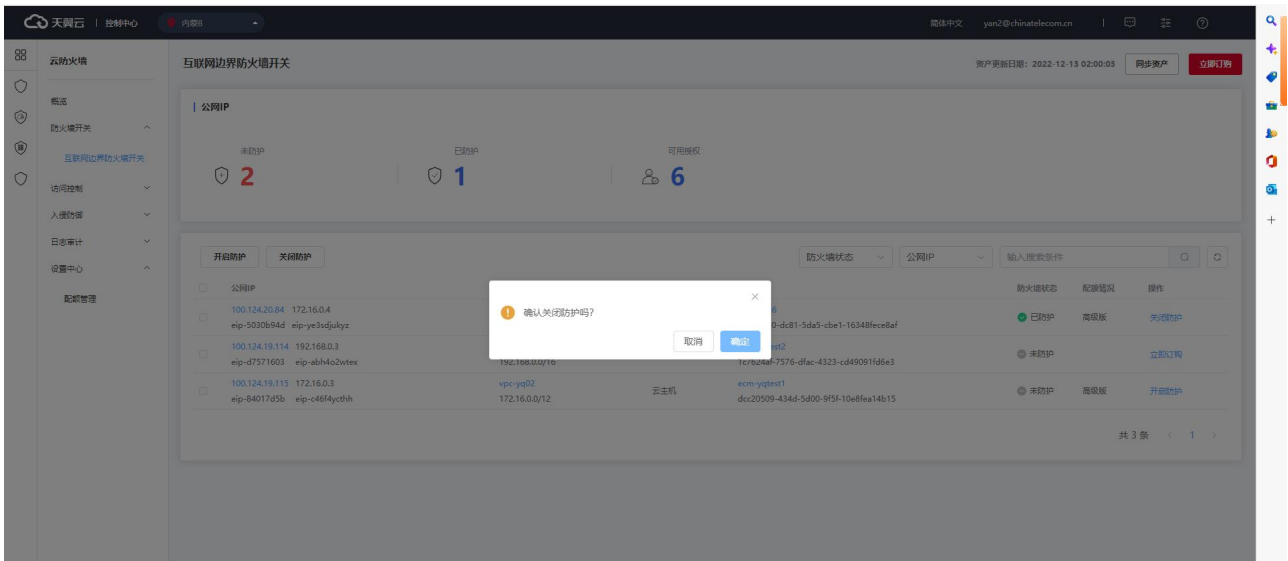
对于已经购买防护配额对应 VPC 中的公网 IP，可进行开启防护和关闭防护。

开启防护时，弹出如下对话框，确定后为该公网 IP 开启防护。



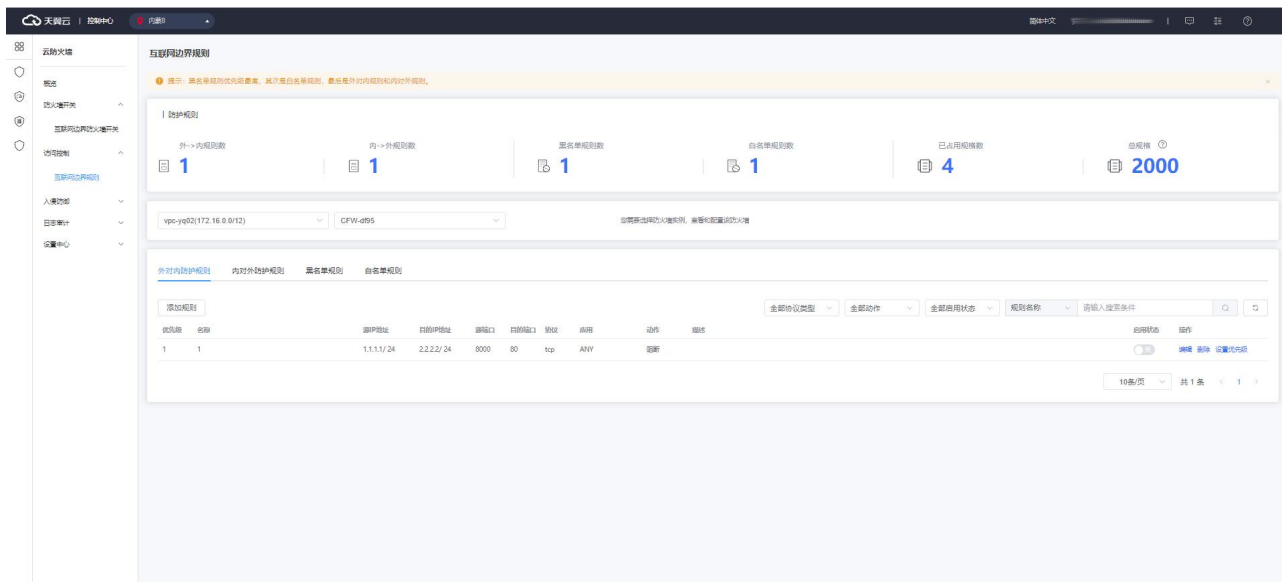


关闭防护时，弹出如下对话框，确定后为该公网 IP 关闭防护。



## 4.4. 访问控制

如下图所示，上方为防护规则统计部分，下方为防护规则列表，分为外->内规则数、内->外规则数、黑名单规则数、白名单规则 4 类，可以根据您的需要分别进行配置。



### 4.4.1. 防护规则概述

本小节介绍了云防火墙（原生版）产品的互联网边界规则统计功能、以及规则优先级。

#### 查看互联网边界规则页面

进入云防火墙（原生版）控制台，在左侧导航栏选择“访问控制 > 互联网边界规则”即可进入互联网边界规则页面。



页面分为两部分：上方为防护规则统计部分，下方为防护规则列表。

- 防护规则统计

对防护规则数量进行统计，包括：黑名单规则数、白名单规则数、外->内规则数、内->外规则数、已占用规格数/总规格。

其中，已占用规格数量=外对内防护规则数+内对外防护规则数+黑名单规则数+白名单规则数，高级套餐中，共包含最多 2000 条访问控制规则，其中外->内规则数、内->外规则数、黑名单规则数、白名单规则数分别不超过 500、500、500、500 条。

- 防护规则列表

防护规则列表包括：黑名单规则、白名单规则、外对内防护规则、内对外防护规则，可以根据您的需要分别进行配置。

### 防护规则优先级

**优先级：**黑名单规则 > 白名单规则 > 外对内防护规则 > 内对外防护规则

防护策略优先级判定顺序的设定为：优先过滤黑名单流量，其次为白名单流量，然后为访问控制策略，最后为入侵防御策略。

1. 为当用户设置黑名单后，此时系统认为黑名单流量即为垃圾流量，系统可根据用户设置的黑名单过滤掉恶意流量，以便系统后续处理非垃圾流量，保证系统处理的数据为用户的有效数据。
2. 当流量经过黑名单过滤后，剩余流量为用户可能关注的流量，在此基础上，通过用户设置的白名单规则，系统可以过滤出用户确定关注的白名单流量，以便对有效流量进行处理，过滤出白名单流量后，系统会直接放行白名单流量至入侵防御策略处进行安全检测，不再进行访问控制。
3. 对于非黑非白的流量，系统将对其进行访问控制检测，对于策略允许的流量进行放行，对于策略禁止的流量进行丢弃。放行后的流量依然需要进行安全检测。

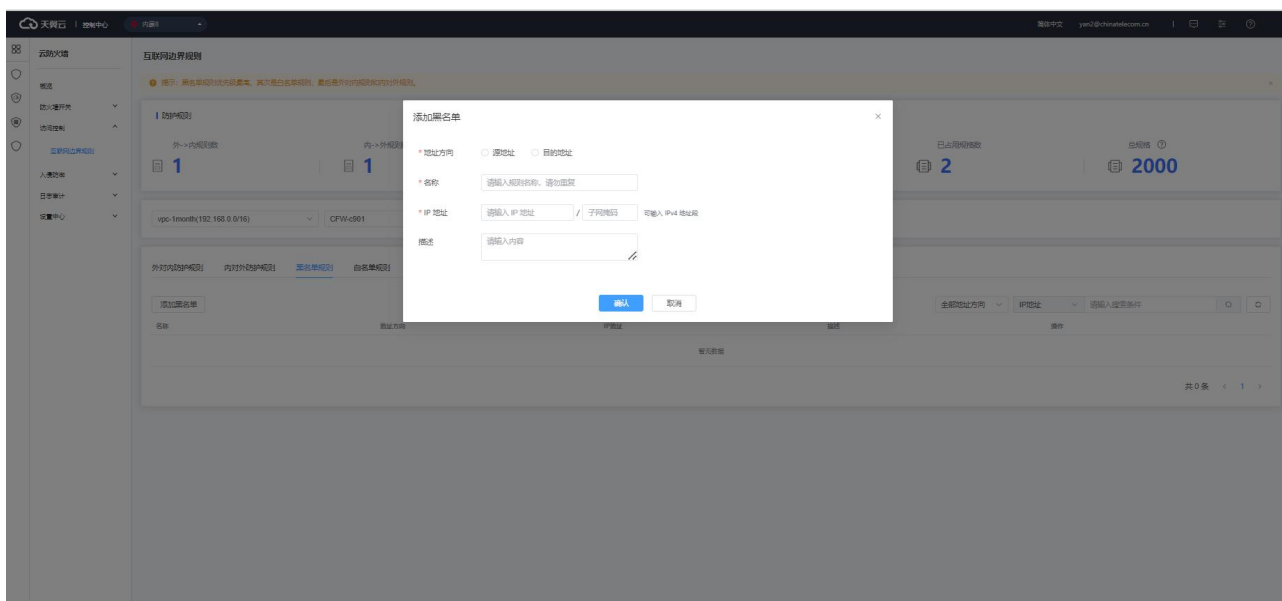
## 4.4.2. 黑名单规则

黑名单规则列表如下图所示，该规则根据您选择的地域和防火墙实例进行展示。选择您需要查看的防火墙实例时，可在下拉列表中选择 VPC 或者防火墙名称均可。



列表包含名称、地址方向、IP 地址、描述和操作。该列表可根据地址方向、源 IP、目的 IP、名称进行筛选。

单击“添加黑名单”，弹出如下对话框：



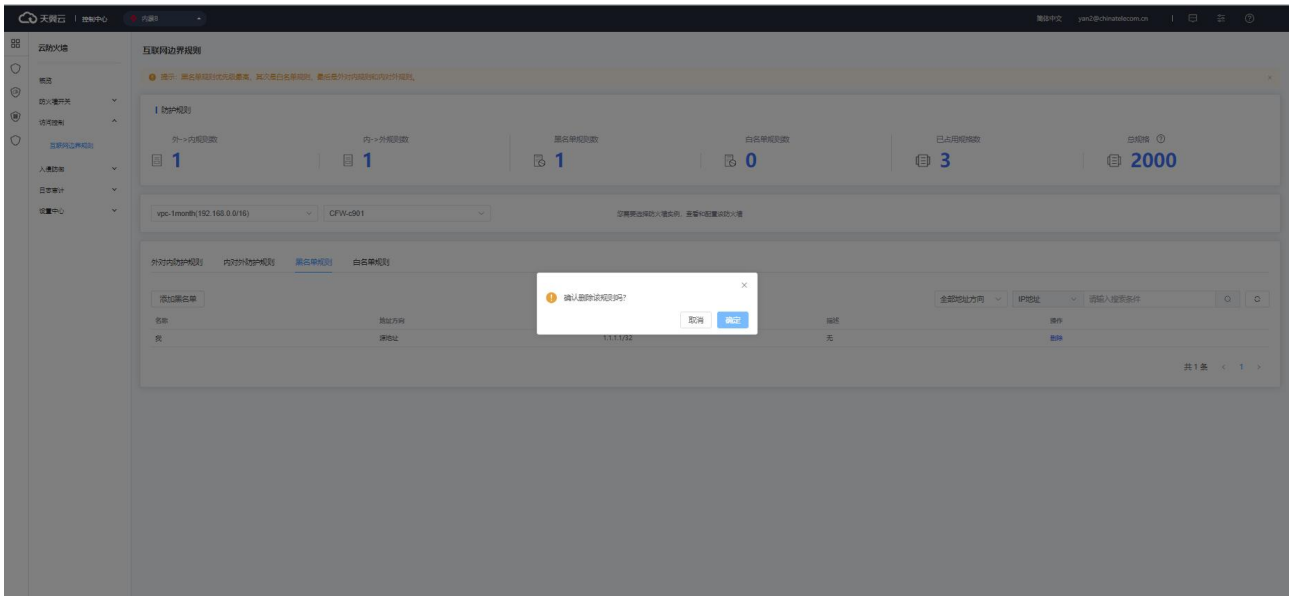
其中，地址方向、名称和 IP 地址为必填，描述为非必填。

地址方向：可选择源地址或目的地址。

名称：输入您为该条黑名单规则命名的名称，中英文均可。

IP 地址：分为 IP 地址和子网掩码，均为必填，可输入 IPv4 单个地址或地址段。

单击黑名单列表操作中的“删除”，弹出下方对话框，确定后删除该黑名单规则，若是取消则关闭对话框。



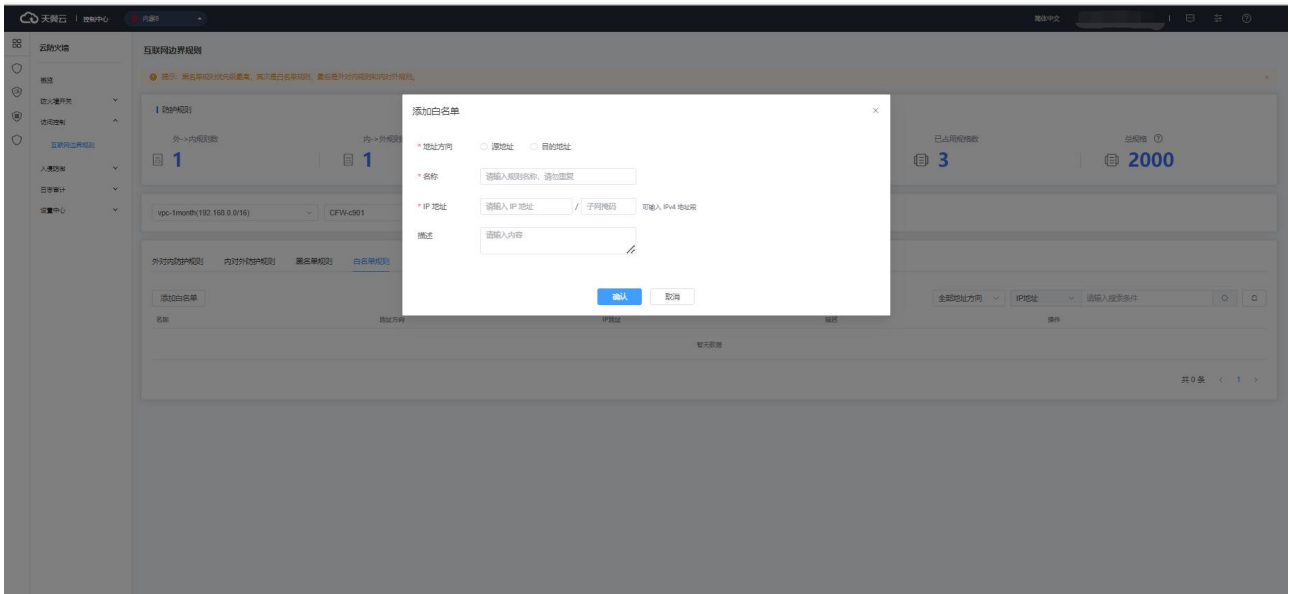
### 4.4.3. 白名单规则

白名单规则列表如下图所示，该规则根据您选择的地区和防火墙实例进行展示。选择您需要查看的防火墙实例时，可在下拉列表中选择 VPC 或者防火墙名称均可。



列表包含名称、地址方向、IP 地址、描述和操作。该列表可根据地址方向、源 IP、目的 IP、名称进行筛选。

单击“添加白名单”，弹出如下对话框：



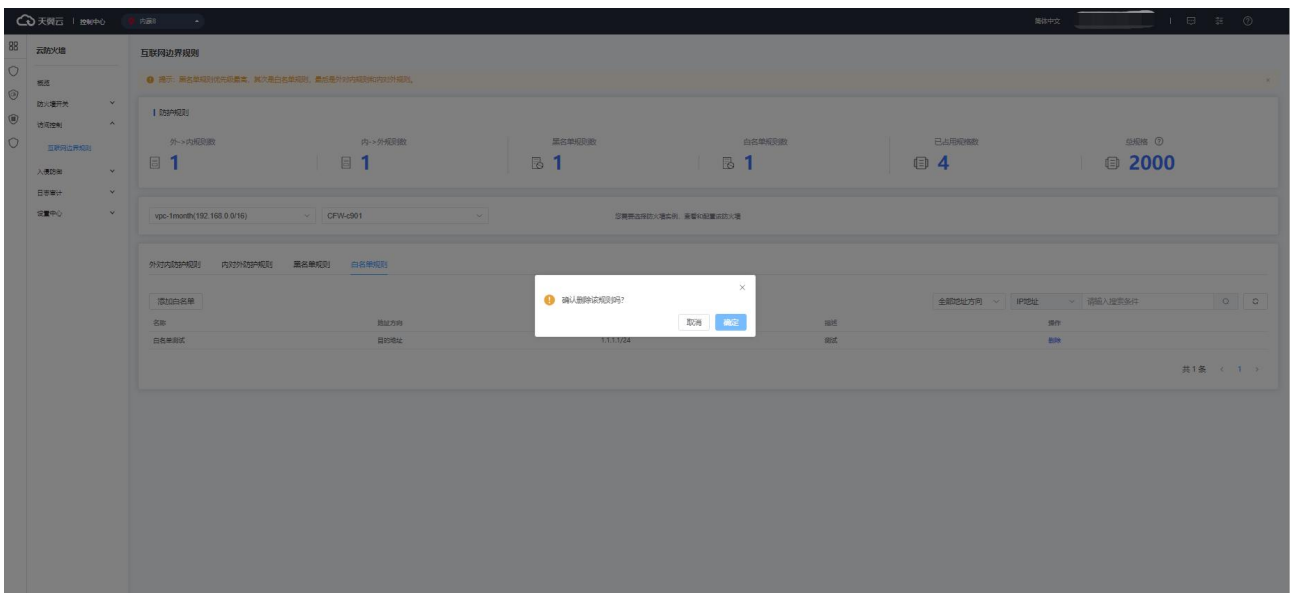
其中，地址方向、名称和 IP 地址为必填，描述为非必填。

地址方向：可选择源地址或目的地址。

名称：输入您为该条白名单规则命名的名称，中英文均可。

IP 地址：分为 IP 地址和子网掩码，均为必填，可输入 IPv4 单个地址或地址段。

单击白名单列表操作中的“删除”，弹出下方对话框，确定后删除该黑名单规则，若是取消则关闭对话框。



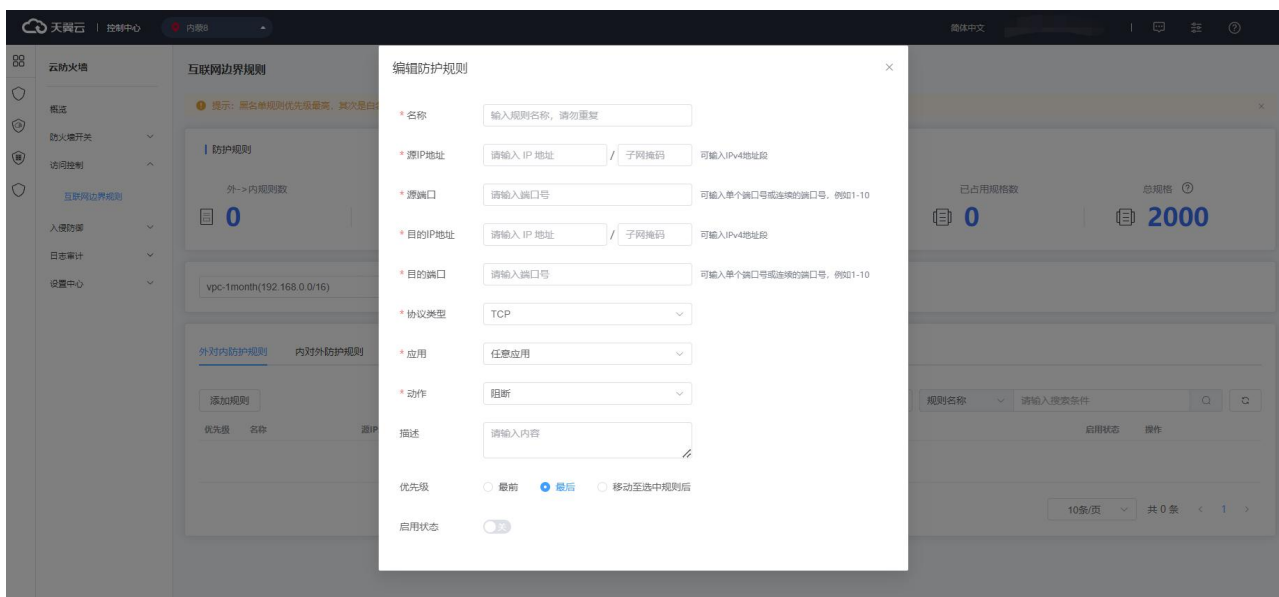
## 4.4.4. 外对内防护规则

外对内防护规则列表如下图所示，该规则根据您选择的地域和防火墙实例进行展示。选择您需要查看的防火墙实例时，可在下拉列表中选择 VPC 或者防火墙名称均可。



外对内防护规则列表包含优先级、名称、源 IP 地址、目的 IP 地址、源端口、目的端口、协议、应用、动作、描述、启用状态和操作。该列表可根据协议类型、动作、启用状态、源 IP、目的 IP、规则名称进行筛选。

单击“添加规则”，进行新的规则添加，如下图所示：



名称、源 IP 地址、源端口、目的 IP 地址、目的端口、协议类型、应用和动作为必填，描述、优先级和启用状态为非必填。

名称：输入您为该条访问控制规则命名的名称，中英文均可。

源 IP 地址：分为 IP 地址和子网掩码，均为必填，可输入 IPv4 单个地址或地址段。

源端口：可输入单个端口号或连续的端口号，例如 1-10 或 80。

目的 IP 地址：分为 IP 地址和子网掩码，均为必填，可输入 IPv4 单个地址或地址段。

目的端口：可输入单个端口号或连续的端口号，例如 1-10 或 80。

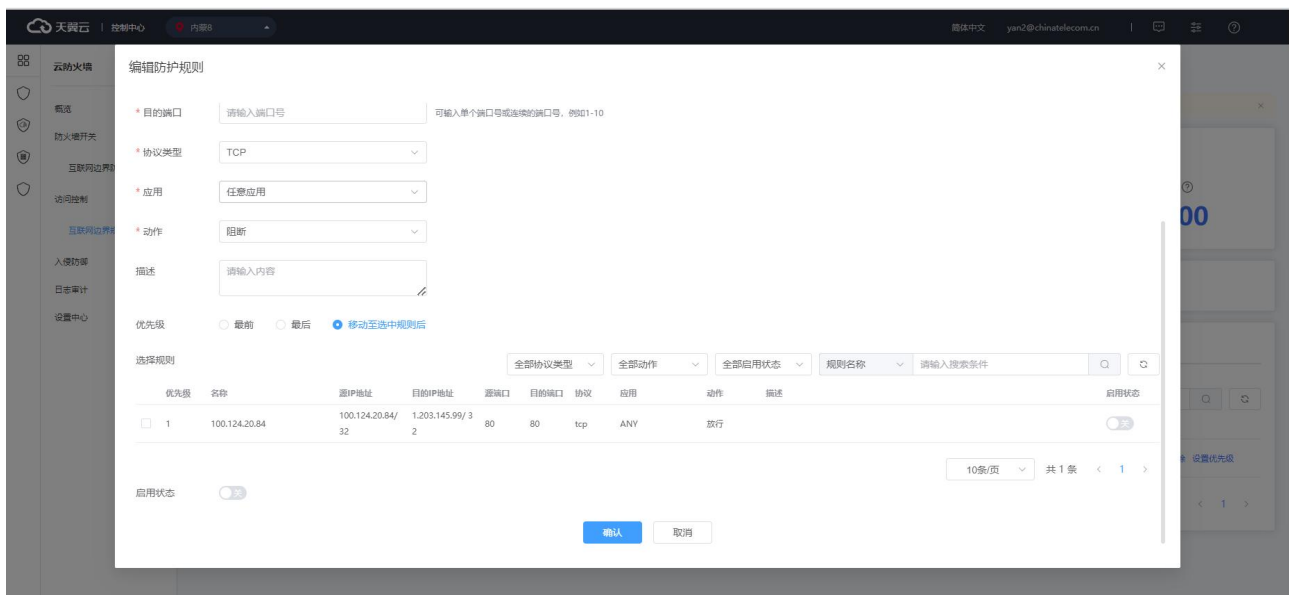
协议类型：可选择 TCP、UDP、ICMP 和 Any 时。

应用：可选择任意应用、MySQL、中国工商银行、维基百科、58 同城、京东商城、滴滴出行、POP3、smtp、ssh、telnet、ftp-data、HTTPS、HTTP、IMAP、TeamViewer、必应和酷狗音乐。

动作：可选择放行或阻断，默认为阻断。

描述：根据情况填写即可。

优先级：默认为最后，也可以选择最前或移动至选中规则后，当选择移动至选中规则后，会展示当前已有的防护规则，选中某条规则后，您当前添加的规则优先级将位于选中的规则之后，如下图所示：

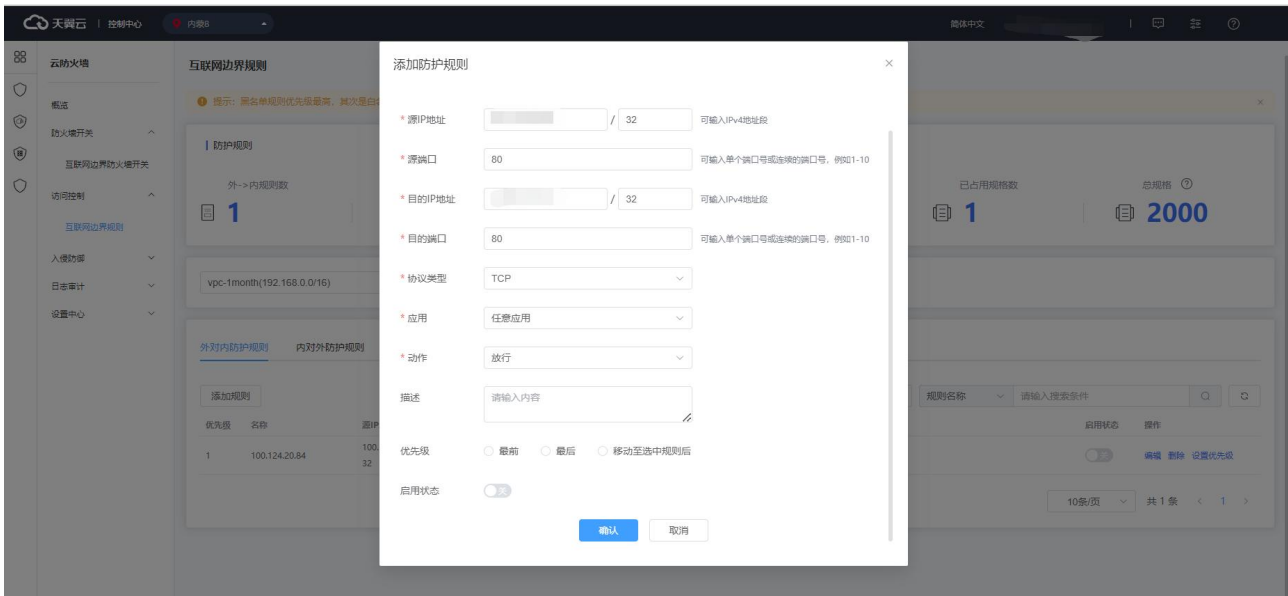


启用状态：默认为关闭，您也可以选择打开。

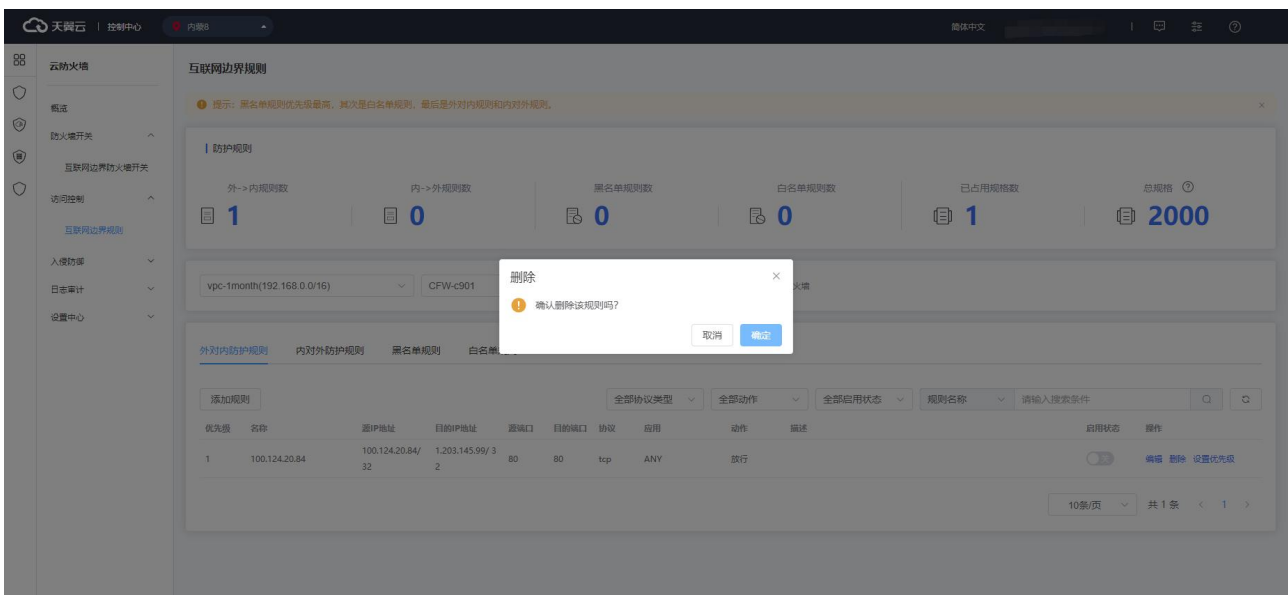
以上所有的字段填写完毕后，点击“确认”时，需要校验这条规则加入后，是否超过客户剩余的规格，若未超过则生成新的外对内访问控制规则。

单击外对内防护规则列表操作中的“编辑”，进行规则编辑，如下图所示：

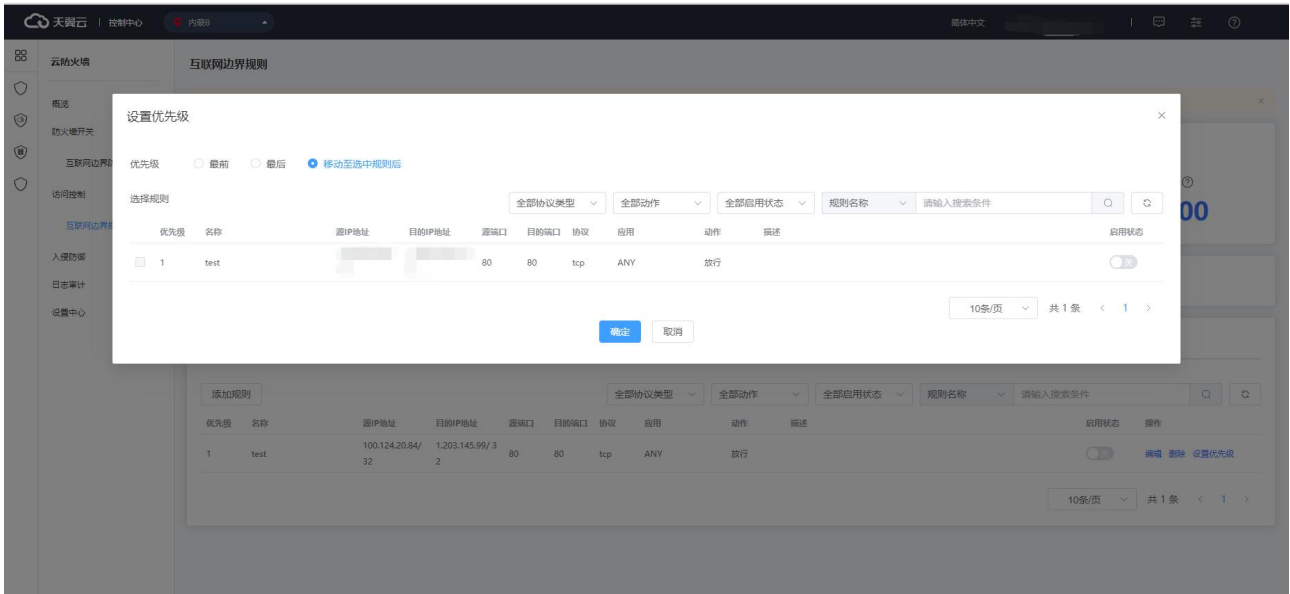




单击外对内防护规则列表操作中的“删除”，进行确认后删除该规则。



单击外对内防护规则列表操作中的“设置优先级”，弹出如下对话框，优先级可以选择最后、最前或移动至选中规则后，当选择移动至选中规则后，会展示当前已有的防护规则，选中某条规则后，您当前添加的规则优先级将位于选中的规则之后。



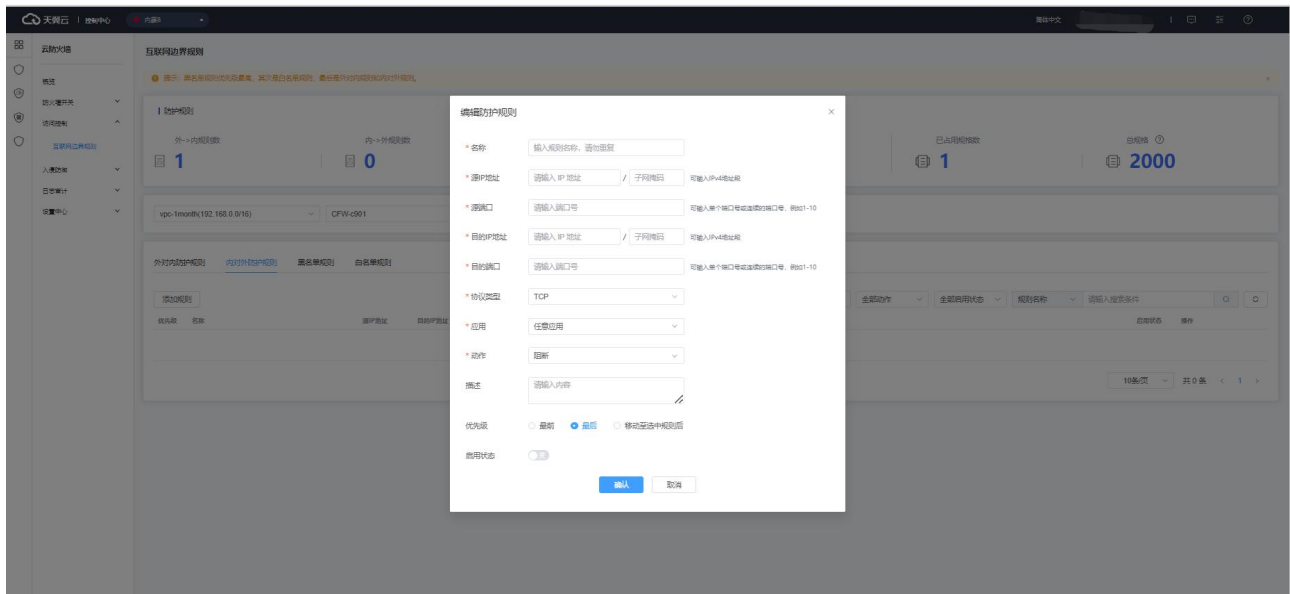
#### 4.4.5. 内对外防护规则

内对外防护规则列表如下图所示，该规则根据您选择的地域和防火墙实例进行展示。选择您需要查看的防火墙实例时，可在下拉列表中选择 VPC 或者防火墙名称均可。



内对外防护规则列表包含优先级、名称、源 IP 地址、目的 IP 地址、源端口、目的端口、协议、应用、动作、描述、启用状态和操作。该列表可根据协议类型、动作、启用状态、源 IP、目的 IP、规则名称进行筛选。

单击“添加规则”，进行新的规则添加，如下图所示：



名称、源 IP 地址、源端口、目的 IP 地址、目的端口、协议类型、应用和动作为必填，描述、优先级和启用状态为非必填。

名称：输入您为该条访问控制规则命名的名称，中英文均可。

源 IP 地址：分为 IP 地址和子网掩码，均为必填，可输入 IPv4 单个地址或地址段。

源端口：可输入单个端口号或连续的端口号，例如 1-10 或 80。

目的 IP 地址：分为 IP 地址和子网掩码，均为必填，可输入 IPv4 单个地址或地址段。

目的端口：可输入单个端口号或连续的端口号，例如 1-10 或 80。

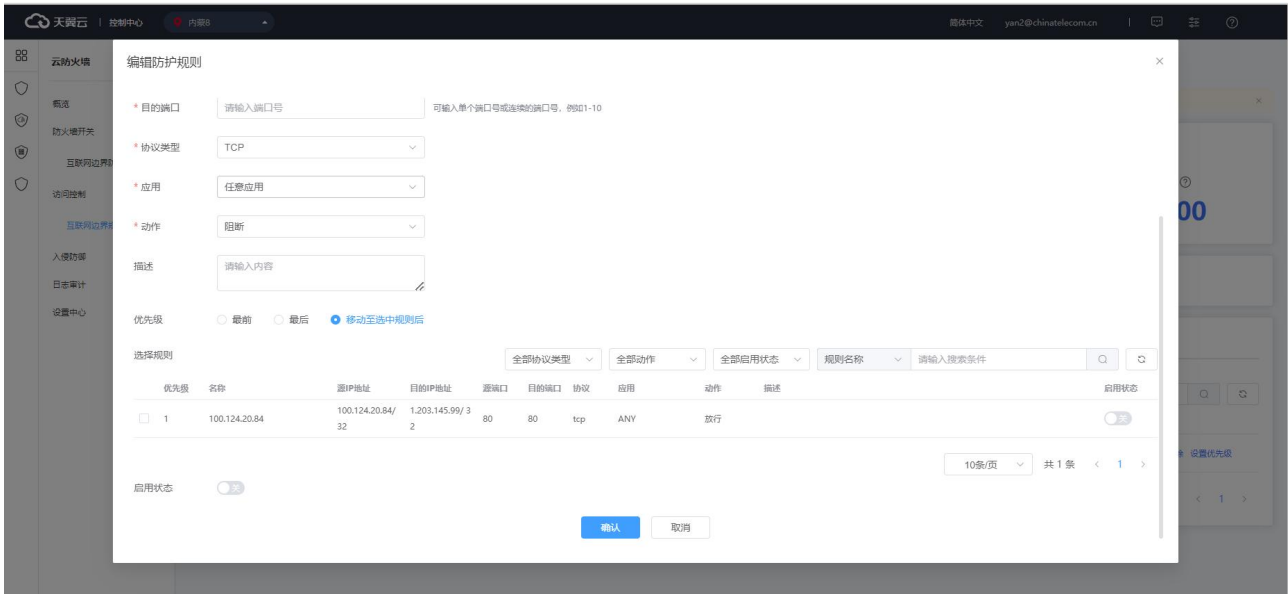
协议类型：可选择 TCP、UDP、ICMP 和 Any 时。

应用：可选择任意应用、MySQL、中国工商银行、维基百科、58 同城、京东商城、滴滴出行、POP3、smtp、ssh、telnet、ftp-data、HTTPS、HTTP、IMAP、TeamViewer、必应和酷狗音乐。

动作：可选择放行或阻断，默认为阻断。

描述：根据情况填写即可。

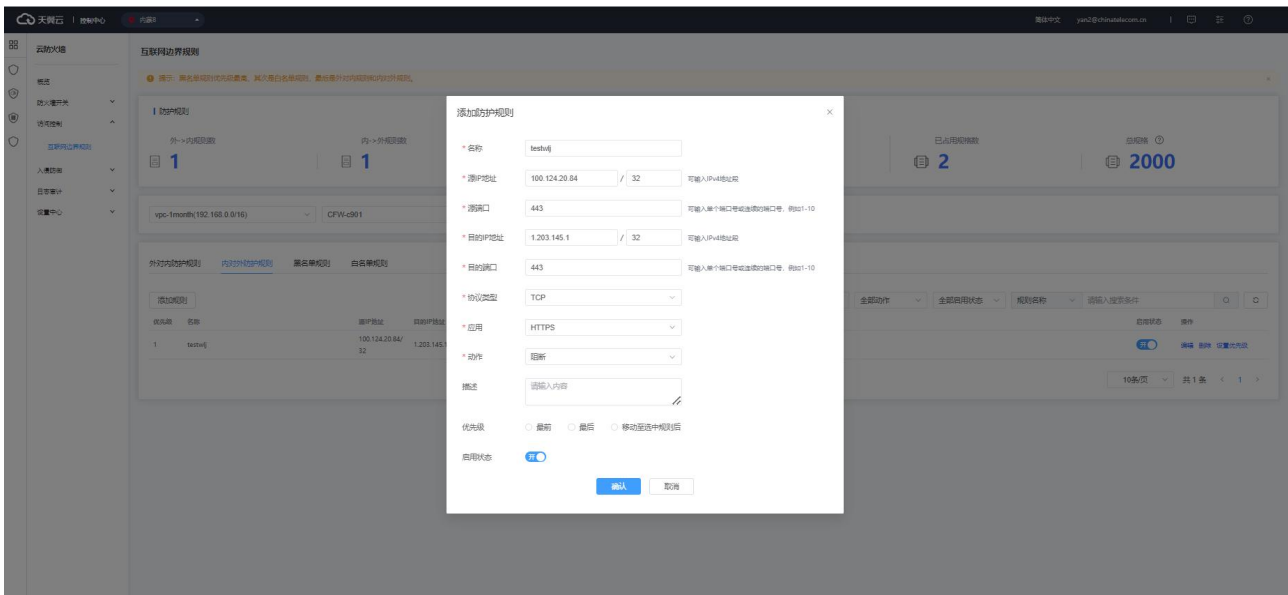
优先级：默认为最后，也可以选择最前或移动至选中规则后，当选择移动至选中规则后，会展示当前已有的防护规则，选中某条规则后，您当前添加的规则优先级将位于选中的规则之后，如下图所示：



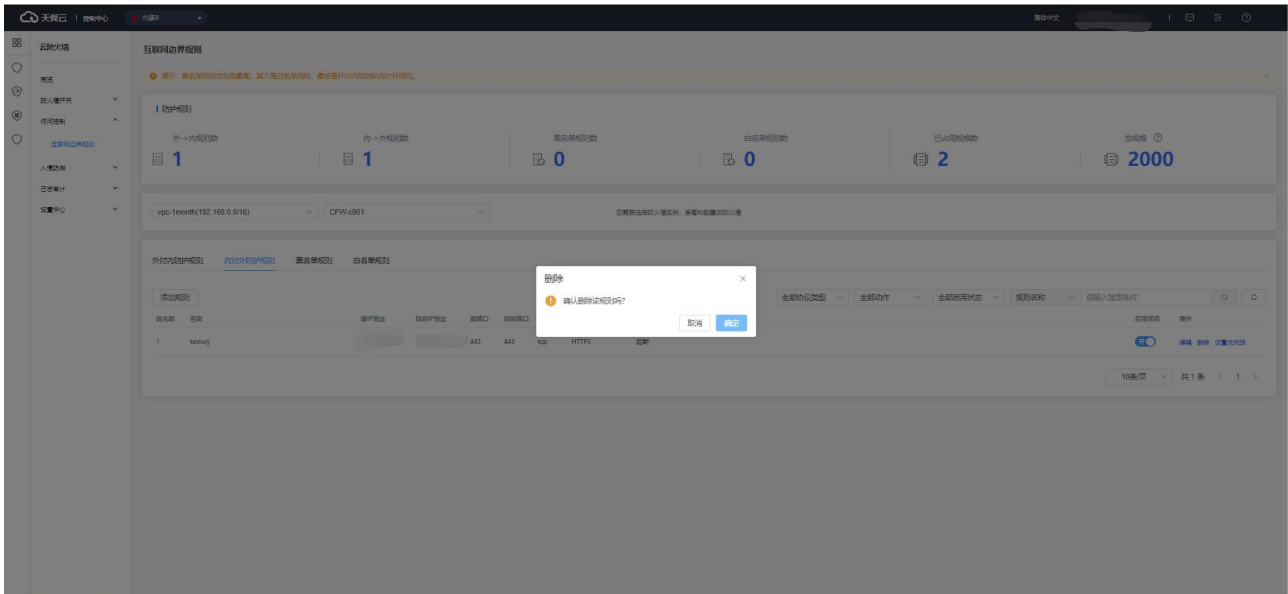
启用状态：默认为关闭，您也可以选择打开。

以上所有的字段填写完毕后，点击“确认”时，需要校验这条规则加入后，是否超过客户剩余的规格，若未超过则生成新的外对内访问控制规则。

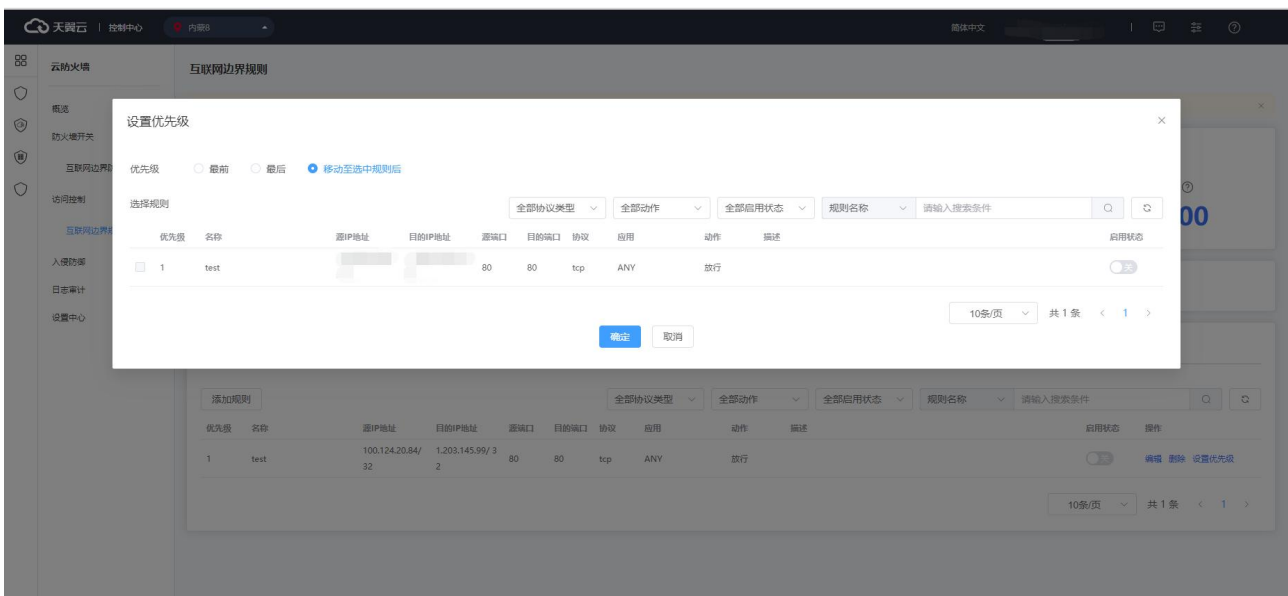
单击内对外防护规则列表操作中的“编辑”，进行规则编辑，如下图所示：



单击内对外防护规则列表操作中的“删除”，进行确认后删除该规则。



单击内对外防护规则列表操作中的“设置优先级”，弹出如下对话框，优先级可以选择最后、最前或移动至选中规则后，当选择移动至选中规则后，会展示当前已有的防护规则，选中某条规则后，您当前添加的规则优先级将位于选中的规则之后。



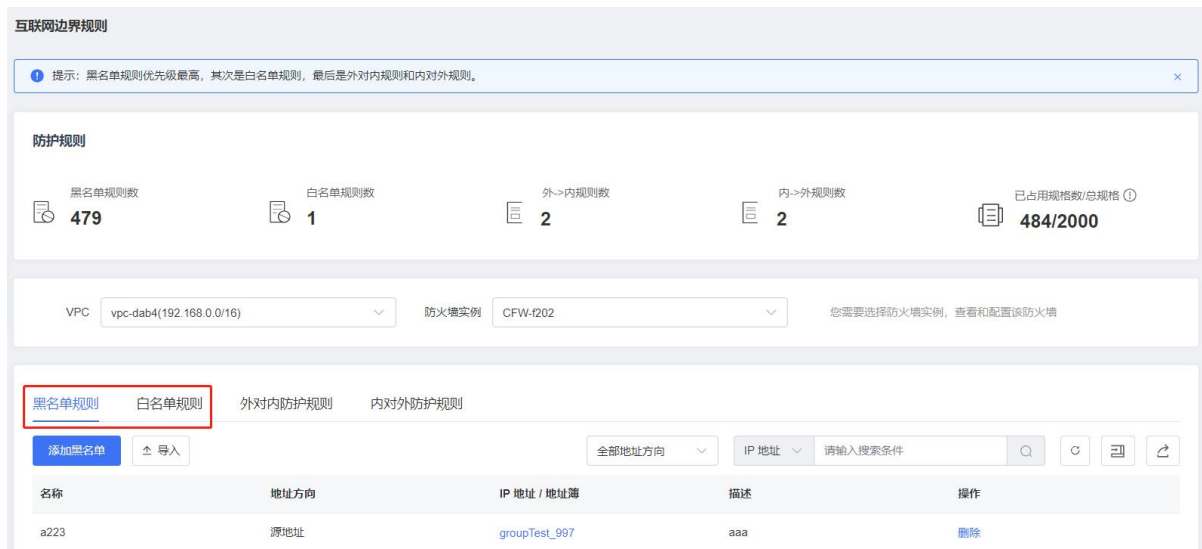
#### 4.4.6. 批量管理黑白名单规则

本小节介绍批量导入和导出黑白名单规则的操作步骤。


##### 进入黑白名单规则页面

1. 登录天翼云控制中心。

2. 单击控制中心顶部的区域选择框，选择区域。
3. 单击控制中心左上角的“服务列表”图标，选择“安全 > 云防火墙（原生版）”。
4. 在左侧导航栏选择“访问控制 > 互联网边界规则”，进入互联网边界规则页面。
5. 选择“黑名单规则”或者“白名单规则”页签，进入相应规则页面。



## 下载黑白名单规则模板

1. 进入黑白名单规则页面。
2. 单击规则列表右上方的下载模板图标，弹出下载模板确认框。
3. 单击“确定”，下载黑白名单规则模板到本地。

## 批量导入黑白名单规则

1. 按表格要求填写您要添加的防护规则信息，防护规则参数说明请参见“导入模板参数说明-黑白名单规则模板”。

注意：


请按照模板要求填写相应参数，确保导入文件的格式与模板一致，否则可能会导入失败。

2. 表格填写完成后，进入目标规则页面，单击规则列表上方的“导入”，弹出导入对话框。



3. 将填写好的表格文件上传到配置文件框。
4. 单击“确定”，导入黑白名单规则表。

### 批量导出黑白名单规则

1. 进入黑白名单规则页面。
2. 单击规则列表右上方的导出表格图标 ，弹出导出表格确认框。
3. 单击“确定”，导出黑白名单规则列表到本地。

### 导入模板参数说明-黑白名单规则模板

参数名称	参数说明
名称	自定义规则名称。名称长度不能超过 100 个字符。
方向	可选择“源地址”或“目的地址”。 <ul style="list-style-type: none"><li>● 源地址：访问流量中的发送数据包的 IP 地址。</li></ul>

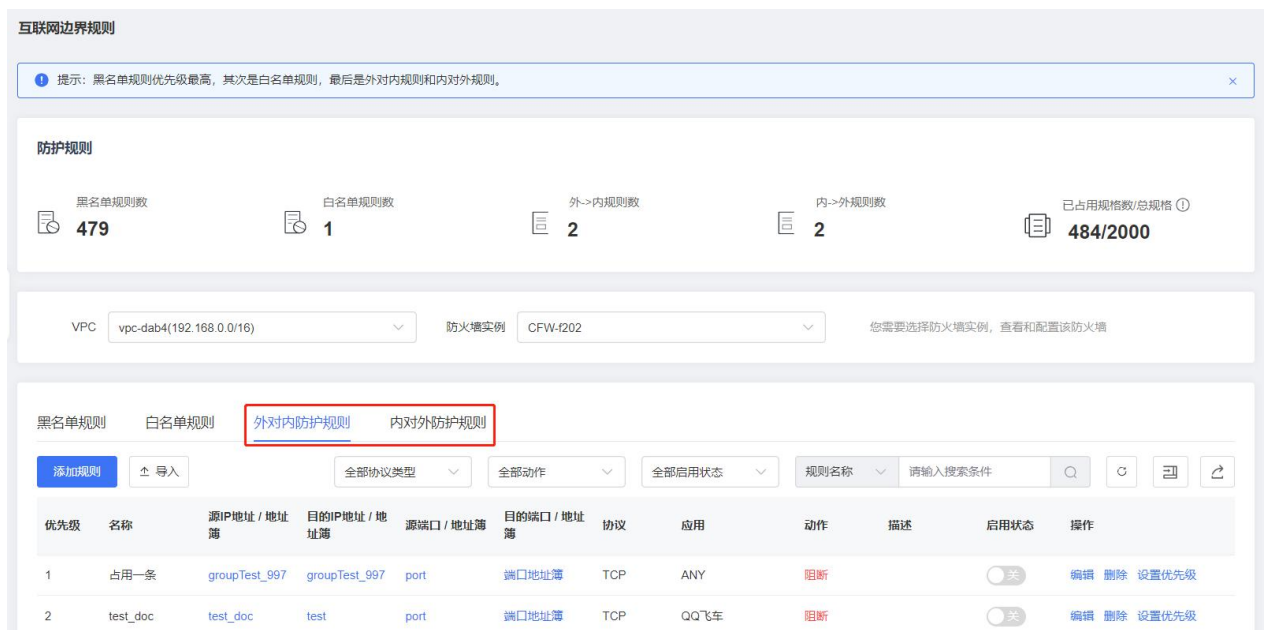
参数名称	参数说明
	<ul style="list-style-type: none"> <li>● 目的地址：访问流量中的接收数据包的 IP 地址。</li> </ul>
IP 地址	支持以下格式： <ul style="list-style-type: none"> <li>● 地址段，使用 “/” 隔开掩码，如：192.168.2.0/24</li> <li>● IP 地址簿名称。IP 地址簿为多个 IPv4 地址的集合，添加 IP 地址簿请参见添加 IP 地址簿。</li> </ul>
描述	自定义规则描述。

## 4.4.7. 批量管理防护规则

本小节介绍批量导入和导出防护规则的操作步骤。

### 进入防护规则页面

1. 登录天翼云控制中心。
2. 单击控制中心顶部的区域选择框，选择区域。
3. 单击控制中心左上角的“服务列表”图标，选择“安全 > 云防火墙（原生版）”。
4. 在左侧导航栏选择“访问控制 > 互联网边界规则”，进入互联网边界规则页面。
5. 选择“外对内防护规则”或者“内对外防护规则”页签，进入相应防护规则页面。



**互联网边界规则**

提示：黑名单规则优先级最高，其次是白名单规则，最后是外对内规则和内对外规则。

**防护规则**

黑名单规则数: 479    白名单规则数: 1    外->内规则数: 2    内->外规则数: 2    已占用规格数/总规格: 484/2000

VPC: vpc-dab4(192.168.0.0/16)    防火墙实例: CFW-f202    您需要选择防火墙实例，查看和配置该防火墙


黑名单规则    白名单规则    **外对内防护规则**    内对外防护规则

添加规则    导入    全部协议类型    全部动作    全部启用状态    规则名称    请输入搜索条件

优先级	名称	源IP地址 / 地址簿	目的IP地址 / 地址簿	源端口 / 地址簿	目的端口 / 地址簿	协议	应用	动作	描述	启用状态	操作
1	占用一条	groupTest_997	groupTest_997	port	端口地址簿	TCP	ANY	阻断		关	编辑 删除 设置优先级
2	test_doc	test_doc	test	port	端口地址簿	TCP	QQ飞车	阻断		关	编辑 删除 设置优先级



### 下载防护规则模板

1. 进入防护规则页面。
2. 单击规则列表右上方的下载模板图标 ，弹出下载模板确认框。
3. 单击“确定”，下载防护规则模板到本地。

### 批量导入防护规则

1. 按表格要求填写您要添加的防护规则信息，防护规则参数说明请参见导入模板参数说明-防护规则模板。

注意：


请按照模板要求填写相应参数，确保导入文件的格式与模板一致，否则可能会导入失败。

2. 表格填写完成后，进入目标防护规则页面，单击防护规则列表上方的“导入”，弹出导入对话框。



3. 将填写好的表格文件上传到配置文件框。
4. 单击“确定”，导入防护规则表。

### 批量导出防护规则

1. 进入防护规则页面。
2. 单击规则列表右上方的导出表格图标 ，弹出导出表格确认框。
3. 单击“确定”，导出防护规则列表到本地。

### 导入模板参数说明 - 防护规则模板

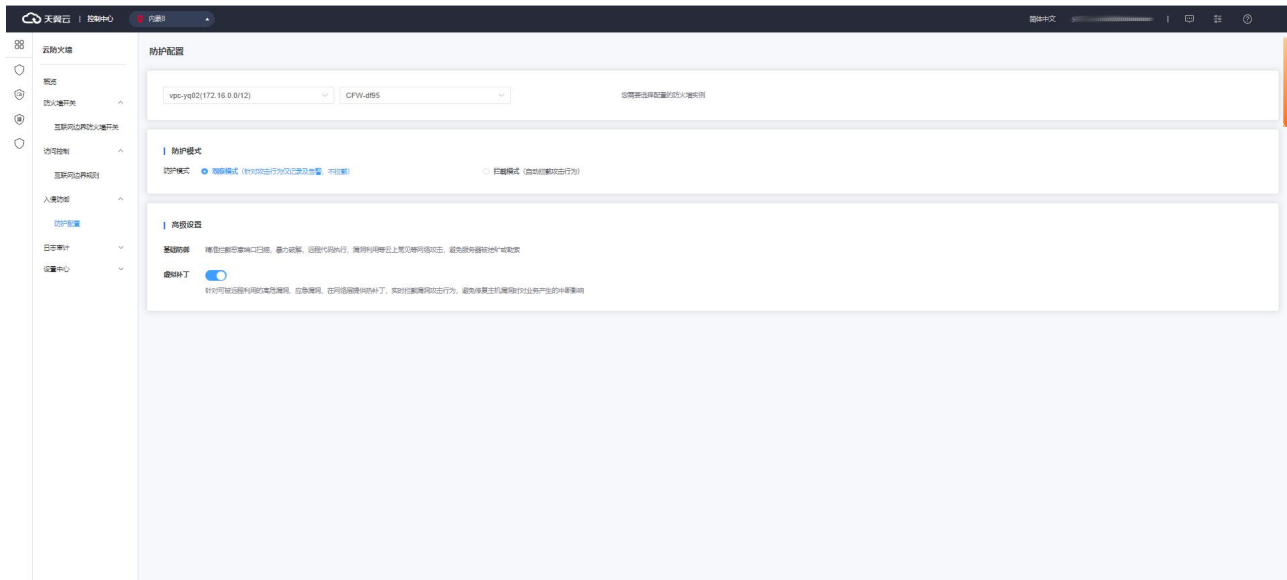
参数名称	参数说明
名称	自定义防护规则名称。名称长度不能超过 100 个字符。
源 IP 地址	支持以下格式： <ul style="list-style-type: none"><li>● 地址段，使用 “/” 隔开掩码，如：192.168.2.0/24</li><li>● IP 地址簿名称。IP 地址簿为多个 IPv4 地址的集合，添加 IP 地址簿请参见添加 IP 地址簿。</li></ul>

参数名称	参数说明
源端口	支持以下格式： <ul style="list-style-type: none"> <li>● 端口号。</li> <li>● 端口地址簿名称。端口地址簿为多个端口的集合，添加端口地址簿请参见添加端口地址簿。</li> </ul>
目的 IP 地址	支持以下格式： <ul style="list-style-type: none"> <li>● 地址段，使用 “/” 隔开掩码，如：192.168.2.0/24</li> <li>● IP 地址簿名称。IP 地址簿为多个 IPv4 地址的集合，添加 IP 地址簿请参见添加 IP 地址簿。</li> </ul>
目的端口	支持以下格式： <ul style="list-style-type: none"> <li>● 端口号。</li> <li>● 端口地址簿名称。端口地址簿为多个端口的集合，添加端口地址簿请参见添加端口地址簿。</li> </ul>
协议类型	支持：TCP、UDP、ICMP、Any。
应用	在下拉框中选择应用，可选择“全部应用”或其中一个应用，包括 MySQL、中国工商银行、维基百科、58 同城、京东商城、滴滴出行、POP3、smtp、ssh、telnet、ftp-data、HTTPS、HTTP、IMAP、TeamViewer、必应和酷狗音乐等。
动作	设置防火墙对流量的处理动作，支持选择“放行”或者“阻断”。
描述	自定义规则描述。
优先级	定义规则优先级。仅支持“最前”或“最后”，若需要移动至选中规则后，请在执行批量导入规则之后再调整规则优先级。
启用状态	选择该规则是否启用规则。 <ul style="list-style-type: none"> <li>● 开：表示启用，规则生效。</li> <li>● 关：表示关闭，规则不生效。</li> </ul>

## 4.5. 入侵防御

### 4.5.1. 防护配置

防护配置页面如下所示：



入侵防御可以进行防护模式选择和高级设置。在配置前您需选择要进行配置的防火墙实例，首先选择地域，其次选择 VPC 或防火墙名称，选择您要设置的防火墙实例。

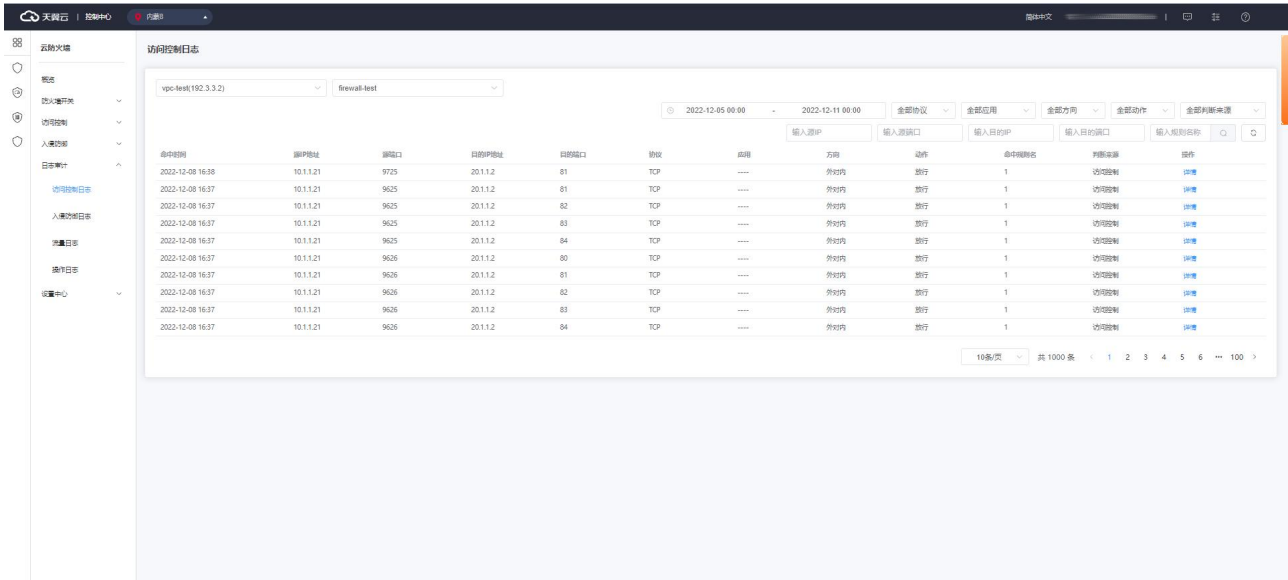
防护模式可选择观察模式和拦截模式。若选择观察模式，则仅针对攻击行为仅记录及告警，不拦截；若选择拦截模式，则自动拦截攻击行为。

高级设置可对虚拟补丁进行打开和关闭设置。

## 4.6. 日志审计

### 4.6.1. 访问控制日志

访问控制日志如下图所示：



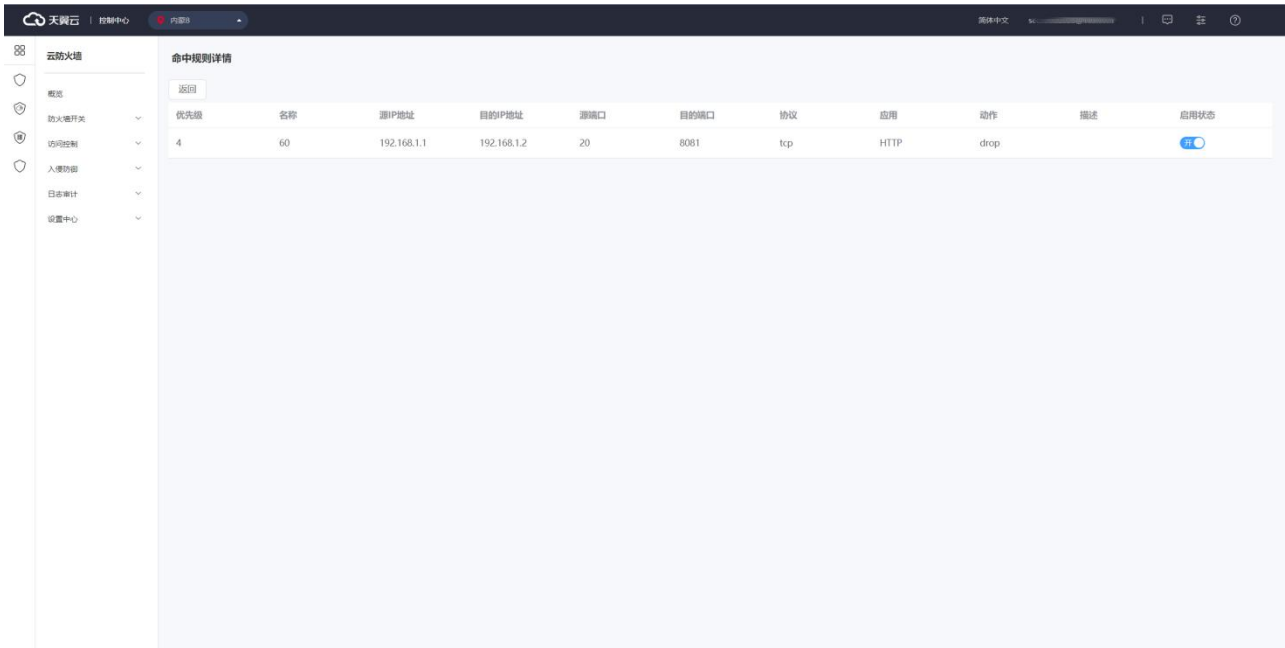
命中时间	源IP地址	源端口	目的IP地址	目的端口	协议	应用	方向	动作	命中规则名	判断来源	操作
2022-12-08 16:38	10.1.1.21	9725	20.1.1.2	81	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9625	20.1.1.2	81	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9625	20.1.1.2	82	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9625	20.1.1.2	83	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9625	20.1.1.2	84	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	80	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	81	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	82	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	83	TCP	---	外对内	放行	1	访问控制	详情
2022-12-08 16:37	10.1.1.21	9626	20.1.1.2	84	TCP	---	外对内	放行	1	访问控制	详情

在查看访问控制日志前，您需选择要进行查看的防火墙实例，首先选择地域，其次选择 VPC 或防火墙名称，选择您要查看的防火墙实例。

访问控制日志列表包括命中时间、源 IP 地址、源端口、目的 IP 地址、目的端口、协议、应用、方向、动作、命中规则名、判断来源和操作。

该列表可根据时间、协议、应用、方向、动作、判断来源、源 IP 地址、源端口、目的 IP 地址、目的端口、规则名称进行搜索和筛选。

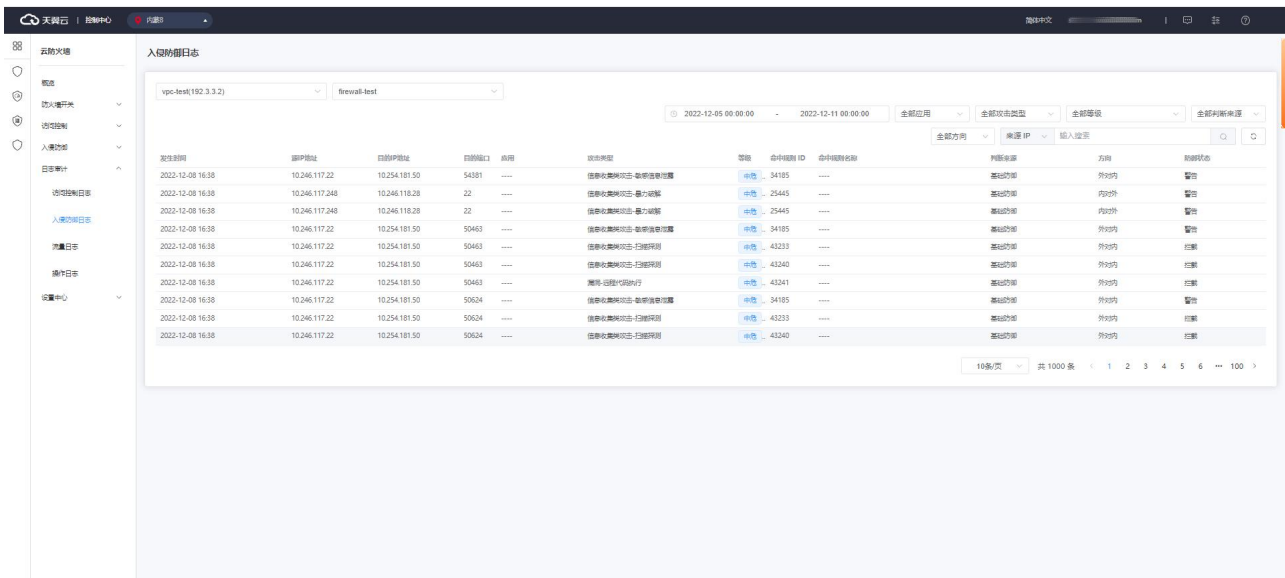
单击操作中的“详情”，跳转至如下页面：



在该页面中，展示了命中规则的优先级、名称、源 IP 地址、目的 IP 地址、源端口、目的端口、协议、应用、动作、描述和启用状态。

## 4.6.2. 入侵防御日志

入侵防御日志如下图所示：



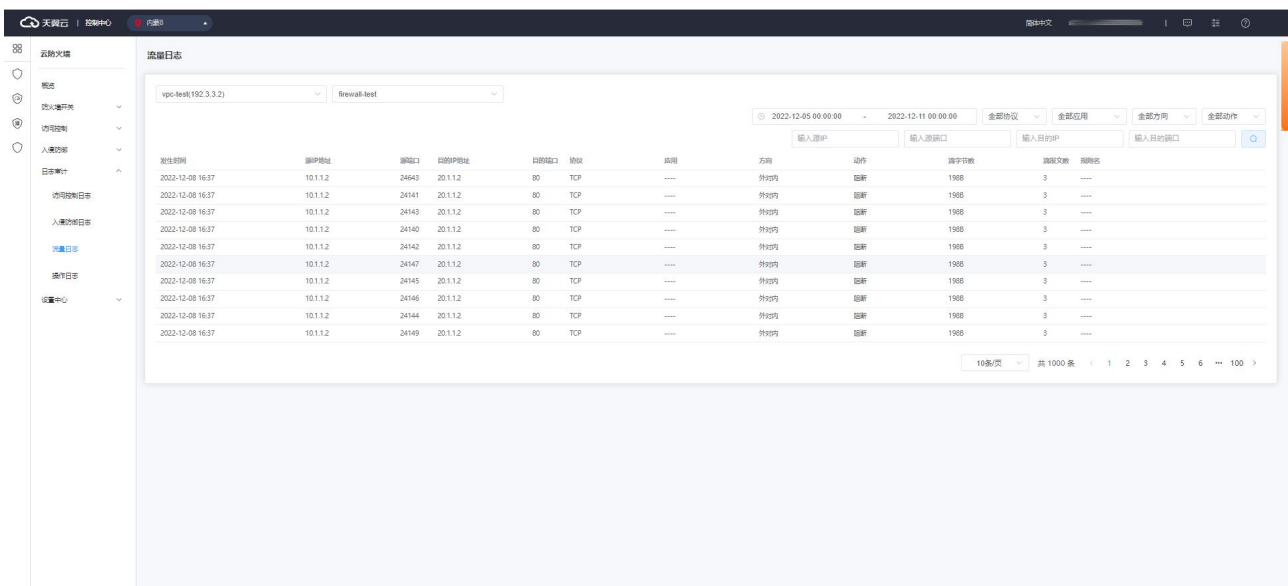
在查看入侵防御日志前，您需选择要进行查看的防火墙实例，首先选择地域，其次选择 VPC 或防火墙名称，选择您要查看的防火墙实例。

入侵防御日志列表包括发生时间、源 IP 地址、目的 IP 地址、目的端口、应用、攻击类型、等级、命中规则 ID、命中规则名称、判断来源、方向和防御状态。

该列表可根据时间、应用、攻击类型、等级、判断来源、方向、来源 IP、目的 IP、进行搜索和筛选。

### 4.6.3. 流量日志

流量日志如下图所示：



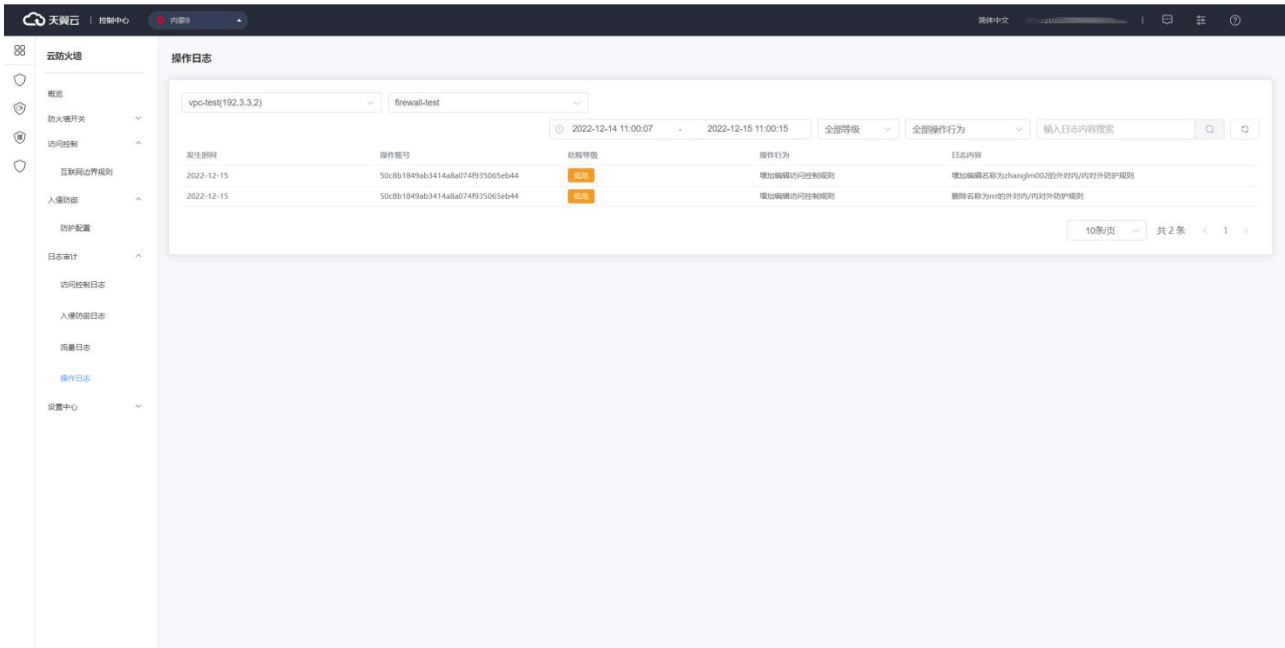
在查看流量日志前，您需选择要进行查看的防火墙实例，首先选择地域，其次选择 VPC 或防火墙名称，选择您要查看的防火墙实例。

流量日志列表包括发生时间、源 IP 地址、源端口、目的 IP 地址、目的端口、协议、应用、方向、动作、流字节数、流报文数、规则名。

该列表可根据时间、协议、应用、方向、动作、源 IP 地址、源端口、目的 IP 地址、目的端口进行搜索和筛选。

### 4.6.4. 操作日志

操作日志如下图所示：



在查看操作日志前，您需选择要进行查看的防火墙实例，首先选择地域，其次选择 VPC 或防火墙名称，选择您要查看的防火墙实例。

操作日志列表包括发生时间、操作账号、危险等级、操作行为、日志内容。

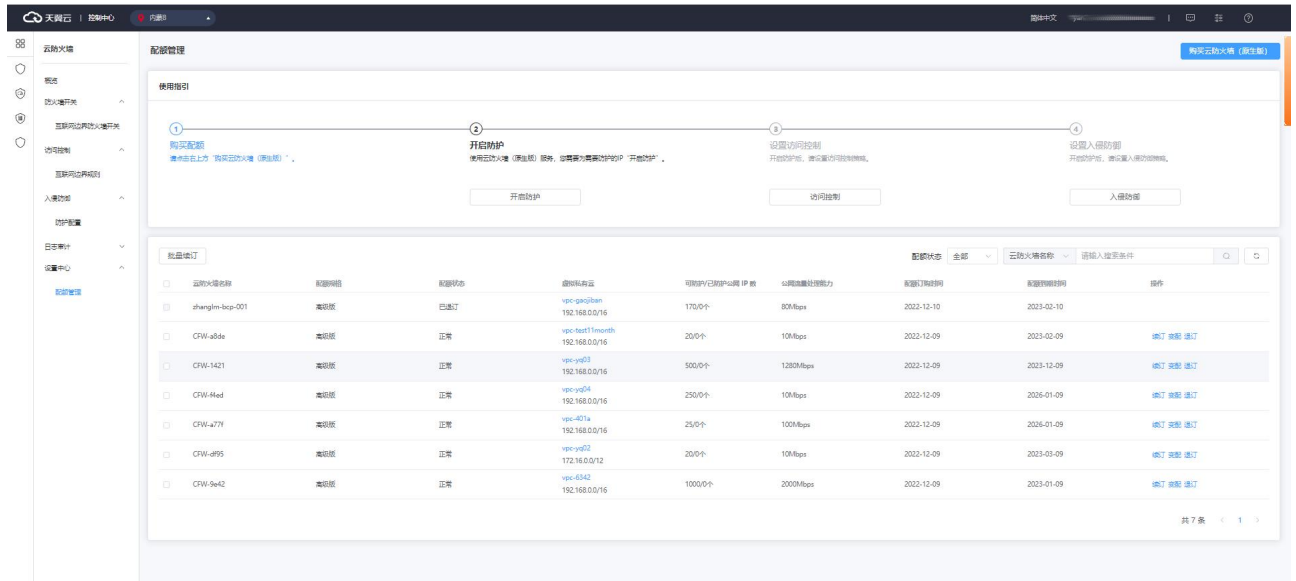
该列表可根据时间、危险等级、操作行为、日志内容进行搜索和筛选。



## 4.7. 设置中心

### 4.7.1. 配额管理

配额管理页面见下图，最上方为您提供云防火墙（原生版）配额订购入口，配额订购具体步骤见 2.2 节；其次展示了使用指引，包括购买配额、开启防护、设置访问控制和设置入侵防御，您可以根据使用步骤去进行操作；下方展示已订购的配额列表。



配额列表展示的范围包括正常、已到期和已退订的配额，已销毁的配额不再展示在列表中。展示列表包括云防火墙名称、配额规格、配额状态、虚拟私有云、可防护/已防护公网 IP 数、公网流量处理能力、配额订购时间、配额到期时间和操作。只有配额状态为“正常”的才可以进行所有操作，配额状态为“已到期”的可以进行续订，配额状态为“已退订”的不可以进行任何操作。该列表可以根据配额状态、云防火墙名称和 VPC 名称去进行查询。

## 4.7.2. 地址簿管理

### 4.7.2.1. IP 地址簿

IP 地址簿是多个 IP 地址的集合。通过使用 IP 地址簿，可帮助用户有效应对需要重复编辑访问规则中 IP 地址的场景，方便批量管理访问规则。

在地址簿列表上方，可通过“地址簿名称”和“IP 地址”对地址簿列表进行筛选。

#### 约束限制

- 每个防火墙实例支持 1000 个地址簿（该配额由 IP 地址簿和端口地址簿共用）。
- 每个地址簿最多支持 1000 个 IP 地址。
- 每个防火墙实例下最多添加 10000 个 IP 地址。

#### 添加 IP 地址簿

1. 登录天翼云控制中心。
2. 单击控制中心顶部的区域选择框，选择区域。
3. 单击控制中心左上角的“产品服务列表”图标，选择“安全 > 云防火墙（原生版）”，进入云防火墙（原生版）的“概览”页面。
4. 在左侧导航栏中，选择“设置中心 > 地址簿管理”，进入“地址簿管理”页面。
5. 在 VPC 和防火墙实例下拉列表中，选择需要配置的防火墙实例。
6. 单击“添加地址簿”，进入“地址簿添加”页面。

地址簿添加
✕

---

**\* 地址簿名称**

可输入中文字符、英文大写字母 (A~Z)、英文小写字母 (a~z)、数字 (0~9) 和特殊字符 (-\_)。长度不超过 255 字符。

**\* 地址簿类型**

**地址簿描述**

0 / 255

可输入中文字符、英文大写字母 (A~Z)、英文小写字母 (a~z)、数字 (0~9) 和特殊字符 (-\_)。

**\* IP 地址**

单个IP地址，如：192.168.10.5。  
地址段，使用"/"隔开掩码，如：192.168.2.0/24。  
多个连续地址，中间使用“-"隔开，如：192.168.0.2-192.168.0.10。  
支持多个输入，使用半角逗号 (,)、半角分号 (;) 或空格隔开，如：  
192.168.1.0,192.168.1.0/24。  
最多支持 1000 个地址

确认

取消

7. 配置地址簿参数，参数说明如下。

参数名称	参数说明
地址簿名称	用户可自定义地址簿名称。 命名规则如下： 可输入中文字符、英文大写字母 (A~Z)、英文小写字母 (a~z)、数字 (0~9) 和特殊字符 (-_)。 长度不超过 255 字符。
地址簿类型	IP 地址簿选择 “IPv4 地址” 。
地址簿描述	用于标识地址簿的用途，以便快速区分不同的地址簿。

参数名称	参数说明
IP 地址	<p>添加该 IP 地址簿需要管理的 IP 地址。最多支持 1000 个地址。</p> <p>支持如下地址格式：</p> <p>单个 IP 地址，如：192.168.10.5。</p> <p>地址段，使用 “/” 隔开掩码，如：192.168.2.0/24。</p> <p>多个连续地址，中间使用 “-” 隔开，如：192.168.0.2-192.168.0.10。</p> <p>支持输入多个 IP 地址，使用半角逗号 (,)、半角分号 (;) 或空格隔开，如：192.168.1.0,192.168.1.0/24。</p>

8. 确认填写信息无误后，单击“确认”，完成添加 IP 地址簿操作。

### 编辑 IP 地址簿

1. 登录天翼云控制中心。
2. 单击控制中心顶部的区域选择框，选择区域。
3. 单击控制中心左上角的“产品服务列表”图标，选择“安全 > 云防火墙（原生版）”，进入云防火墙（原生版）的“概览”页面。
4. 在左侧导航栏中，选择“设置中心 > 地址簿管理”，进入“地址簿管理”页面。
5. 在 VPC 和防火墙实例下拉列表中，选择需要配置的防火墙实例。
6. 找到目标地址簿，单击目标地址簿操作列的“详情”。
7. 在详情页面可以查看地址簿“基本信息”和 IP 地址列表。



- 添加 IP 地址

在 IP 地址列表上方，单击“添加”，弹出添加 IP 地址页面，添加 IP 地址后，单击“确认”，完成添加操作。

- 编辑 IP 地址

在 IP 地址列表的操作列，单击“编辑”，修改 IP 地址。

- 删除 IP 地址

在 IP 地址列表的操作列，单击“删除”，删除 IP 地址。

### 删除 IP 地址簿

注意：

- 使用中的地址簿无法删除，删除地址簿前请先从防护规则中移除地址簿。
- 删除地址簿后无法恢复，请谨慎操作。

1. 登录天翼云控制中心。
2. 单击控制中心顶部的区域选择框，选择区域。
3. 单击控制中心左上角的“产品服务列表”图标，选择“安全 > 云防火墙（原生版）”，进入云防火墙（原生版）的“概览”页面。
4. 在左侧导航栏中，选择“设置中心 > 地址簿管理”，进入“地址簿管理”页面。
5. 在 VPC 和防火墙实例下拉列表中，选择需要配置的防火墙实例。
6. 找到需要删除的地址簿，单击目标地址簿操作列的“删除”。
7. 在弹出的确认框中，单击“确定”，完成删除。

#### 相关操作

IP 地址簿在防护规则里设置后才会生效，添加防护规则请参见：

- [黑名单规则](#)
- [白名单规则](#)
- [外对内防护规则](#)
- [内对外防护规则](#)

### 4.7.2.2. 端口地址簿

端口地址簿是多个端口的集合。通过使用端口地址簿，可帮助用户有效应对需要重复编辑访问规则中端口的场景，方便批量管理访问规则。

在地址簿列表上方，可通过“地址簿名称”和“IP 地址”对地址簿列表进行筛选。

## 约束限制

- 每个防火墙实例支持 1000 个地址簿（该配额由 IP 地址簿和端口地址簿共用）。
- 每个地址簿最多支持 50 个端口。

## 添加端口地址簿

1. 登录天翼云控制中心。
2. 单击控制中心顶部的区域选择框，选择区域。
3. 单击控制中心左上角的“服务列表”图标，选择“安全 > 云防火墙（原生版）”，进入云防火墙（原生版）的“概览”页面。
4. 在左侧导航栏中，选择“设置中心 > 地址簿管理”，进入“地址簿管理”页面。
5. 在 VPC 和防火墙实例下拉列表中，选择需要配置地址簿的防火墙实例。
6. 单击“添加地址簿”，进入“地址簿添加”页面。

## 地址簿添加



\* 地址簿名称

请输入地址簿名称

可输入中文字符、英文大写字母 (A~Z)、英文小写字母 (a~z)、数字 (0~9) 和特殊字符 (-\_)。长度不超过 255 字符。

\* 地址簿类型

端口

地址簿描述

请输入地址簿描述

0 / 255

可输入中文字符、英文大写字母 (A~Z)、英文小写字母 (a~z)、数字 (0~9) 和特殊字符 (-\_)。

\* 端口

单个端口，如：80多个连续端口，中间使用“-”隔开，如：80-443。  
支持多个输入，使用半角逗号 (,)、半角分号 (;) 或空格隔开，如：80,82-443。  
最多支持 50 个端口。

确认

取消

### 7. 配置地址簿参数，参数说明如下。

参数名称	参数说明
地址簿名称	<p>用户可自定义地址簿名称。</p> <p>命名规则如下：</p> <ul style="list-style-type: none"> <li>● 可输入中文字符、英文大写字母 (A~Z)、英文小写字母 (a~z)、数字 (0~9) 和特殊字符 (-_)。</li> <li>● 长度不超过 255 字符。</li> </ul>
地址簿类型	<p>端口地址簿选择“端口”。</p>



参数名称	参数说明
地址簿描述	用于标识地址簿的用途，以便快速区分不同的地址簿。
端口	<p>添加该端口地址簿需要管理的端口。最多支持 50 个端口。</p> <p>支持如下格式：</p> <ul style="list-style-type: none"> <li>● 单个端口，如：80。</li> <li>● 多个连续端口，中间使用“-” 隔开，如：80-443。</li> <li>● 支持输入多个端口，使用半角逗号（,）、半角分号（;）或空格隔开，如：80,82-443。</li> </ul>

8. 确认填写信息无误后，单击“确认”，完成添加端口地址簿操作。

### 编辑端口地址簿

1. 登录天翼云控制中心。
2. 单击控制中心顶部的区域选择框，选择区域。
3. 单击控制中心左上角的“服务列表”图标，选择“安全 > 云防火墙（原生版）”，进入云防火墙（原生版）的“概览”页面。
4. 在左侧导航栏中，选择“设置中心 > 地址簿管理”，进入“地址簿管理”页面。
5. 在 VPC 和防火墙实例下拉列表中，选择需要配置的防火墙实例。
6. 找到目标地址簿，单击目标地址簿操作列的“详情”。
7. 在详情页面可以查看地址簿“基本信息”和端口列表。



- 添加端口

在端口列表上方，单击“添加”，弹出添加端口页面，添加端口后，单击“确认”，完成添加操作。

- 编辑端口

在端口列表的操作列，单击“编辑”，修改端口。

- 删除端口

在端口列表的操作列，单击“删除”，删除端口。

### 删除端口地址簿

**注意：**

- 使用中的地址簿无法删除，删除地址簿前请先从防护规则中移除地址簿。
- 删除地址簿后无法恢复，请谨慎操作。

1. 登录天翼云控制中心。
2. 单击控制中心顶部的区域选择框，选择区域。
3. 单击控制中心左上角的“产品服务列表”图标，选择“安全 > 云防火墙（原生版）”，进入云防火墙（原生版）的“概览”页面。
4. 在左侧导航栏中，选择“设置中心 > 地址簿管理”，进入“地址簿管理”页面。
5. 在 VPC 和防火墙实例下拉列表中，选择需要配置的防火墙实例。
6. 找到需要删除的地址簿，单击目标地址簿操作列的“删除”。
7. 在弹出的确认框中，单击“确定”，完成删除。

### **相关操作**

端口地址簿在防护规则里设置后才会生效，添加防护规则请参见：

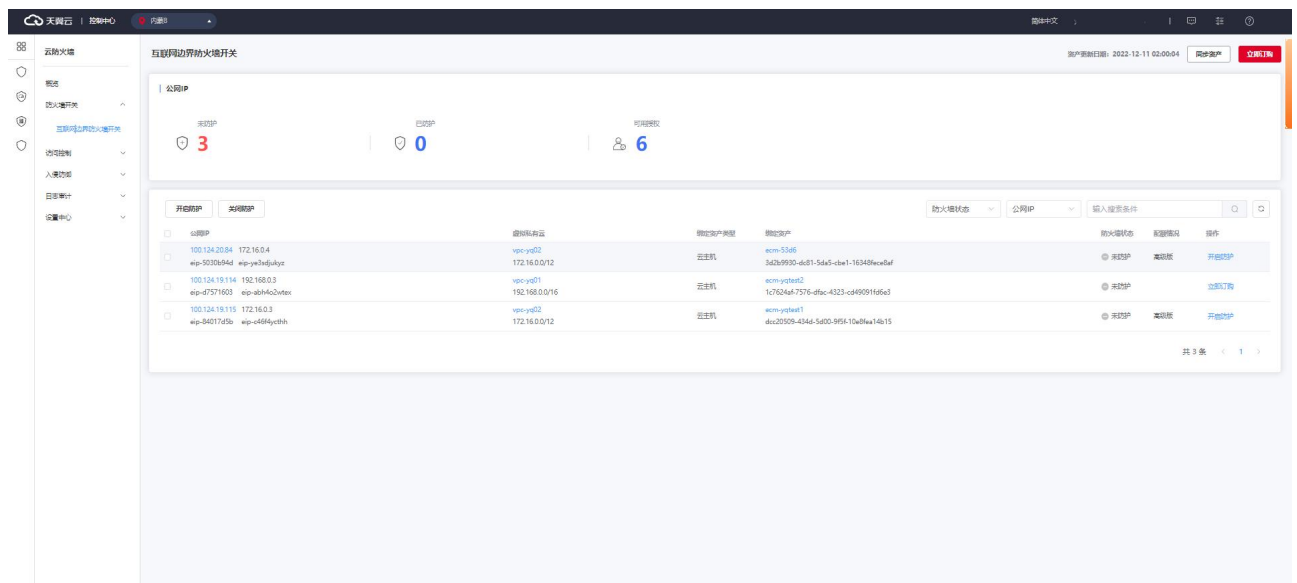
- [外对内防护规则](#)
- [内对外防护规则](#)

# 5. 最佳实践

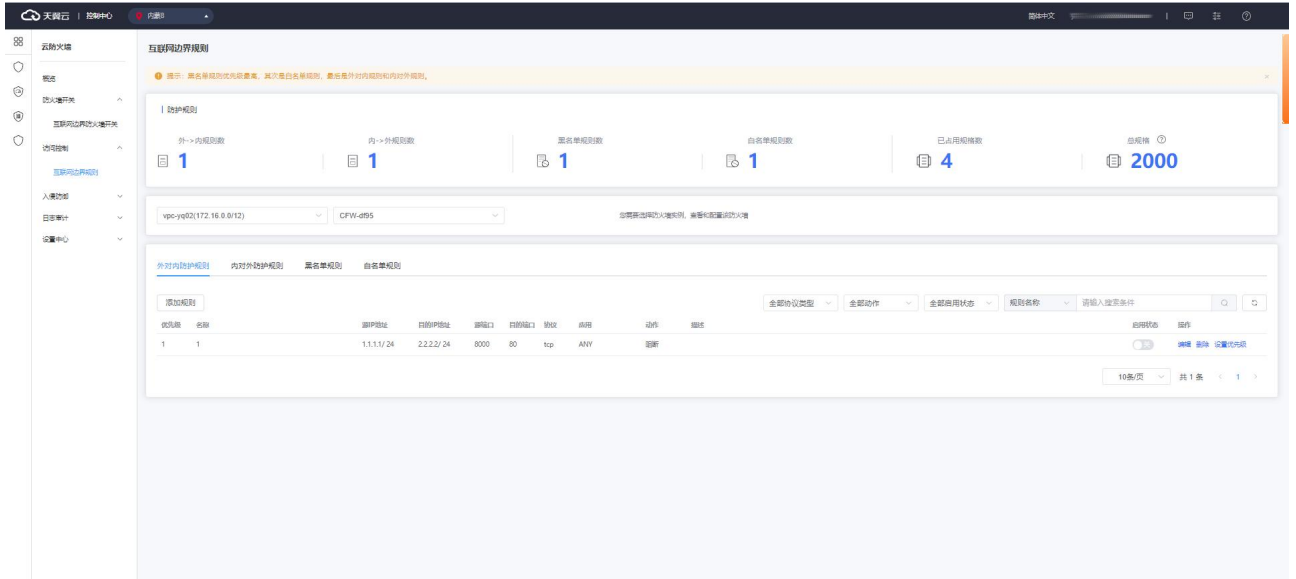
## 5.1. 云防火墙最佳实践

本节从 EIP 防护带宽选择、开启资产保护、配置访问控制策略等方面提供指导。

1. 如何选择适合我的 EIP 防护带宽：云防火墙目前只有高级版，支持 EIP 防护带宽 10M~2000M，建议 EIP 防护带宽不小于 VPC 内 EIP 总带宽；
2. 开启公网资产保护：互联网边界防火墙帮助您检测和防护云上公网 IP 资产间的通信流量。只有为资产开启互联网边界防火墙后，您才可以使用云防火墙分析和控制云上主机的互联网访问流量；您可以在“防火墙开关->互联网边界防火墙开关”页面，对指定的公网 IP 资产开启互联网边界防火墙，如下图所示：

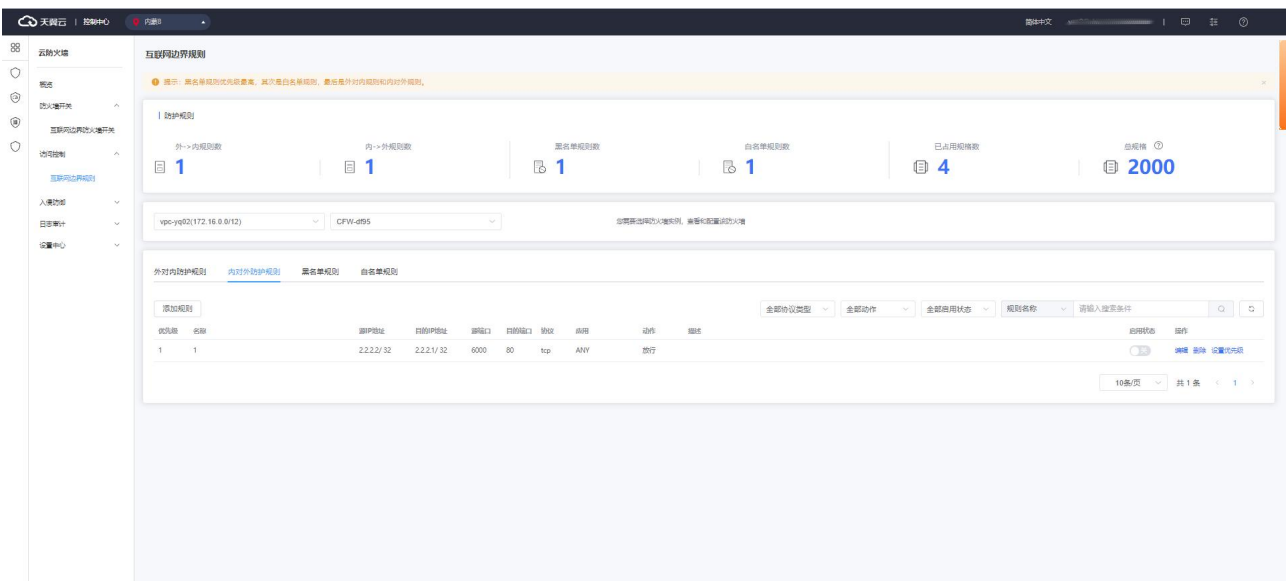


3. 配置外到内的访问策略：在“访问控制->互联网规则->外对内防护规则”页面可进行配置，如下图所示：



在外对内流量的访问策略中，不要对公网 IP 全部端口开放访问，对外仅开放必要的互联网 IP 和端口，其他端口请全部设置为拒绝。放行需要对外开放的应用或端口。在访问控制页面外对内流量列表中，依据业务需求，将源 IP 地址配置为 0.0.0.0/0 或特定源，也可选择地址簿中系统默认配置的地址簿 ANY（0.0.0.0/0）或特定源，目的选择要放开的 IP 或地址簿中的特定目的，协议选择 ANY 或者依据业务需要选择对应协议，动作选择放行。例如，80 端口为 Web 服务，对全网开放，因此访问源为 0.0.0.0/0；1433、3389 端口分别为 SqlServer、RDP 服务，对特定源开放，因此访问源为特定源。将除放行策略之外的流量设置为拒绝放行。在访问控制页面外对内流量列表中，将源 IP 地址配置为 0.0.0.0/0 或地址簿中系统默认配置的地址簿 ANY（0.0.0.0/0），目的设置为 ANY，协议设置为 ANY，动作选择拒绝。

4. 配置内到外的访问策略：在“访问控制->互联网规则->内对外防护规则”页面可进行配置，如下图所示：



内对外流量建议不要开放全部放行的策略，只对到必要的外部 IP 的访问开启放行，其他访问全部设置为拒绝。放行需要对外访问的应用或端口。在访问控制页面内对外流量列表中，依据业务需求，将源 IP 地址配置为 0.0.0.0/0 或特定源，也可选择地址簿中系统默认配置的地址簿 ANY (0.0.0.0/0) 或特定源，目的选择要放开的域名或 IP 或地址簿中的特定目的，协议选择 ANY 或者依据业务需要选择对应协议，动作选择放行。将除放行策略之外的流量设置为拒绝放行。在访问控制页面内对外流量列表中，将源 IP 地址配置为 0.0.0.0/0 或选择地址簿中系统默认配置的地址簿 ANY (0.0.0.0/0)，目的设置为 ANY，协议设置为 ANY，动作选择拒绝。

## 5.2. 配置访问控制策略最佳实践

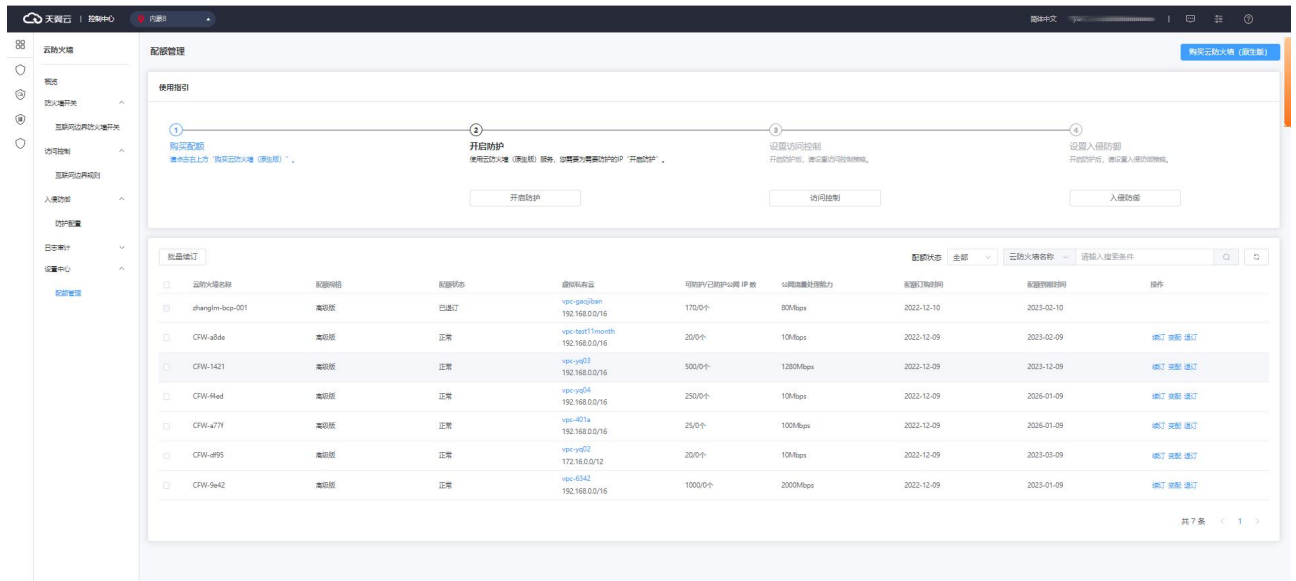
本节介绍互联网边界防火墙访问控制策略的推荐配置方法。

原理：在互联网到所有云上资产的公网出入路径进行统一访问控制。

默认策略：默认全部放行。

推荐配置步骤：

1. 登录云防火墙控制台。在左侧导航栏，选择“访问控制->互联网边界规则”，如下图所示：



2. 在互联网边界规则页面，配置互联网外对内流量。放行所有在互联网开放的必要端口，比如 http (80)、https (443) 服务等。有限放行运维或高安全风险的端口，比如 ssh (22)、mysql (3306) 等端口。默认禁止互联网的高危服务端口，比如 smb (445) 端口等。配置 Any 到 Any 的默认放行策略，启用状态为开，配合流量日志观察无误后再切换启用状态为关。
3. 验证策略是否满足需求。在“日志审计->流量日志”处查询所有流量放行、阻断，可以结合实际测试结果验证策略是否满足要求。

4. 完善互联网边界访问控制策略。验证没有误拦截情况后，可以考虑将 Any 到 Any 的默认策略的启用状态从开切换到关。注意：此步骤需要评估风险后再操作。
5. 检查所有业务的可用性。在“日志审计->流量日志”页面，查询所有流量放行、阻断情况，可以结合实际测试结果验证策略是否满足要求。
6. 配置主动外联访问控制策略（内对外流量）。请参考以下配置逻辑：对主动外联有访问控制需求时，可以在“访问控制->互联网规则->内对外防护规则”处配置。
7. 推荐只放行到特定目的 IP 的请求。默认拦截其它所有主动外联流量（可以先观察一段时间确认所有外联需求）。

## 6. 常见问题

### 6.1. 产品类

**Q: 云防火墙（原生版）与 Web 应用防火墙（原生版）有什么区别？**

**A:** Web 应用防火墙（原生版）针对 Web 业务防护，对非 Web 类业务没有防护能力，且只防护由外对内的攻击。对业务的恶意主动外联没有监测和防护能力。

云防火墙（原生版）包含全部业务防护，支持对 Web 漏洞的基础防护，同时支持内对外的主动外联流量检测。支持失陷主机和恶意外联的自动拦截。

类别	云防火墙	Web 应用防火墙
产品定义	云防火墙（原生版）（CT-CFW, Cloud Firewall）一款云原生的云上边界网络安全防护产品，可提供统一的互联网边界管控与安全防护，并提供业务整体情况可视化、日志审计和分析等功能，帮助您完成网络边界防护与等保合规	Web 应用防火墙（原生版）（CT-WAF, Web Application Firewall）为用户 Web 应用提供一站式安全防护，对 Web 业务流量进行智能全方位检测，有效识别恶意请求特征并防御，避免源站服务器被恶意入侵，保护网站核心业务安全和数据安全
防护对象	IP（弹性公网 IP、内网 IP 等）	域名
网络层级	四层	七层
应用场景	边界网络防护	Web 业务安全防护
核心技术	ACL 访问控制、DPI 深度包检测、IPS 入侵检测技术	HTTP 协议解析、web 攻击检测
安全能力	支持外部访问控制和主动外联管控，能够检测攻击者对用户网络发起的攻击，同时也能对用户网络主动外联行为进行分析，阻断由内而外的恶意连接行为，保护用户的资产安全	集成机器学习检测引擎，支持专家经验特征与语义特征，有效检测 SQL 注入、XSS 等基于形式语言的攻击类型，对 OWASP 常见攻击类型进行了良好覆盖

Web 应用防火墙建议使用场景：

当用户部署了对外提供服务的 Web 应用时，建议用户购买 Web 应用防火墙，以便能够保护所部署 Web 服务的安全。



注意：

无论所部署的 Web 服务是否位于天翼云上，都可以购买天翼云 Web 应用防火墙（原生版）对用户的 Web 服务提供防护，天翼云 Web 应用防火墙（原生版）提供全球级服务，能够为用户任意位置的 Web 服务提供全面的 Web 安全保护。

云防火墙建议使用场景：

当用户在天翼云上购买了弹性云主机时，建议购买云防火墙，以便能够保护用户云上弹性云主机的安全。

注意：

天翼云云防火墙仅能保护部署在天翼云内的弹性云主机网络安全，对于在其他位置的主机和网络设备，因其网络流量未流经天翼云，故天翼云云防火墙无法保护其网络安全。

**Q：天翼云云防火墙（原生版）都支持哪些资源池的防护？**

A：目前天翼云云防火墙（原生版）支持防护的资源池为华东 1，其他资源池还在努力加载中，敬请期待。

**Q：云防火墙有 QPS 限制么？**

A：云防火墙是 SaaS 化服务，通过 ACL 控制策略对用户的网络流量访问进行控制，为云上用户的网络提供边界网络防护，支持用户便捷的弹性扩张，区别于传统防火墙的硬件化部署模式，云防火墙不受硬件性能上限的制约，故对传统硬件防火墙的并发、新建、QPS 等均不限制，只限制防护互联网边界访问的流量峰值。

注意：

当用户互联网边界的流量超过防火墙防护的上限时，防火墙会直接转发超过峰值的流量，此时，该部分流量将不受防火墙访问控制策略及安全策略的防护。故建议用户在进行防火墙服务购买时，充分评估流量峰值情况，并准备部分冗余规格，以便有效保证互联网边界在安全防护下，购买方式请参见订购。当用户在使用过程中，因业务扩展，导致已经购买的产品规格不能满足业务的需要时，可提前对防火墙规格进行规划和扩张，变配方式请参见变配。

**Q：云防火墙支持其他云的服务器吗？**

A：不支持，因防火墙设备属于四层的网络设备，其防护原理为通过对网络流量的访问控制及安全检测防护对用户的网络进行防护，故需要将用户的网络流量引流至防火墙设备，才能对对应的流量进行防护。而云防火墙是云原生的云上边界网络安全防护产品，主要用于云上网络的边界安全防护，通过云内网络路由及引流，将云内网络流量引流至云上防火墙，从而实现对云上网络设备的安全防护，故对于非本云上的服务器以及云下的硬件服务器，由于其网络流量未流经天翼云，不能对其进行安全防护。

注意：

若用户购买了天翼云弹性云主机，并且部署需要联通互联网的云业务，建议用户一定要购买天翼云云防火墙对相关业务进行防护，以便保证该云业务免受来源于网络的恶意攻击。

#### Q：云防火墙的防护策略顺序是什么？

A：云防火墙的防护策略的顺序为：黑名单规则->白名单规则->外对内规则和内对外规则->入侵防御规则。

说明：

防火墙防护策略优先级判定顺序的设定为优先过滤黑名单流量，其次为白名单流量，然后为访问控制策略，最后为入侵防御策略。其设定原因如下：

- 为当用户设置黑名单后，此时系统认为黑名单流量即为垃圾流量，系统可根据用户设置的黑名单过滤掉恶意流量，以便系统后续处理非垃圾流量，保证系统处理的数据为用户的有效数据。
- 当流量经过黑名单过滤后，剩余流量为用户可能关注的流量，在此基础上，通过用户设置的白名单规则，系统可以过滤出用户确定关注的白名单流量，以便对有效流量进行处理，过滤出白名单流量后，系统会直接放行白名单流量至入侵防御策略处进行安全检测，不再进行访问控制。
- 对于非黑非白的流量，系统将对其进行访问控制检测，对于策略允许的流量进行放行，对于策略禁止的流量进行丢弃。放行后的流量依然需要进行安全检测。

#### Q：云防火墙和安全组之间有什么区别？

A：**安全组**：安全组是一种网络安全防护机制，用于防止未经授权的访问和保护计算机网络免受恶意攻击。它是一种虚拟防火墙，用于限制入向和出向网络流量通行。安全组工作在网络层和传输层，它通过检查数据包的源地址、目标地址、协议类型和端口号等信息来决定是否允许通过。安全组创建后，用户可以在安全组中定义各种访问规则，当弹性云主机加入该安全组后，即受到这些访问规则的保护。安全组是

用于云主机之间访问控制的一种安全策略，用户可以通过设置安全组规则，去控制云服务器的出入向流量。通过配置适当的规则，控制和保护加入安全组的弹性云服务器的访问。

**云防火墙：**提供统一的互联网边界管控与安全防护，并提供业务整体情况可视化、日志审计和分析等功能，完成网络边界防护与等保合规需求，主要用于用户虚拟网络中的 ECS 与互联网之间安全防护，支持外部访问控制欲主动外联管控，在进行访问控制的同时，还支持入侵防御，帮助用户建立边界网络防护基石。

## 6.2. 计费类

**Q：云防火墙（原生版）计费方式是什么？**

A：云防火墙（原生版）为包周期计费，分为按月和按年 2 种方式。

**Q：云防火墙（原生版）计费项是什么？**

A：云防火墙（原生版）的计费项为服务版本、流量扩展项、IP 扩展项和购买时长。

**Q：云防火墙（原生版）的配额续费条件是什么？**

A：您所需续费的配额，需要为未到期或已到期状态。

**Q：哪些流量会占用云防火墙的防护带宽？**

A：云防火墙的防护带宽为公网到您防火墙所在 VPC 间的互访流量。

## 6.3. 购买类

**Q：云防火墙（原生版）可以按天购买吗？**

A：不支持，目前只支持包月和包年购买。

**Q：云防火墙的流量带宽和防护 IP 数支持升降吗？**

A: 支持。但在降配时，每次只支持降级一个参数，即防护互联网边界的流量峰值、防护互联网边界公网 IP 数若都要降配，需要分两个订单完成。

**Q: 支持同时防护公网的 IP 不够要怎么办?**

A: 高级版可通过弹性扩展提升规格，可按照您的需要进行 IP 升配。

## 6.4. 操作类

**Q: 未配置任何访问控制规则时，云防火墙默认规则是放行还是拦截?**

A: 云防火墙（原生版）默认阻断防护 IP 的所有流量，您需要将放行的流量进行访问控制规则配置，从而进行放通。未防护 IP 不受影响。

**Q: 入侵防御拦截模式什么时候开?**

A: 一般从观察告警模式切换到阻断拦截模式，业务没有变化，观察 1-2 天即可持续开启。

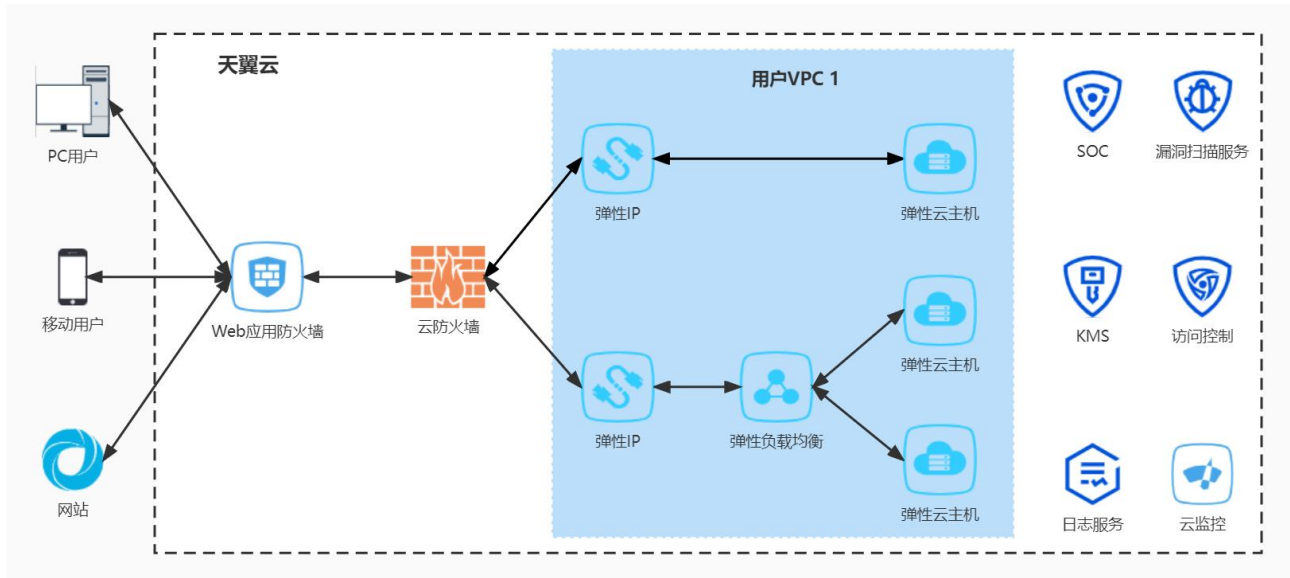
**Q: 入侵防御拦截模式开启后，是否会影响到云内网地址间的通信?**

A: 不会。拦截模式开启后，只会影响云上业务的互联网流量，不会影响到云内网地址间的通信。

## 6.5. 系统类

**Q: 云防火墙（原生版）在天翼云网络中的位置是什么?**

A: 如下图所示，云防火墙一般和 DDoS 防护系统、Web 应用防火墙、数据中心网络、日志服务、SOC 等一起组合使用，但也可以独立部署。DDoS 防护系统、Web 应用防火墙和云防火墙组成从外到内的三道屏障，云防火墙重点防护用户 VPC 的网络边界。云防火墙产生的日志通过日志服务来收集和对外展示，通过 SOC 整合汇聚（包括云防火墙在内的）各安全设备的日志和安全告警等，并结合外部威胁情报，可以提高安全数据利用率并挖掘潜在威胁，对抗愈发复杂的攻击手段与高级可持续威胁。



**Q: 云防火墙（原生版）是否可以防护非天翼云上的资产？**

A: 防火墙仅能防护天翼云账号下的 IP 资产，不支持非天翼云的资产。

**Q: 云防火墙（原生版）支持防护哪些资产类型？**

A: 目前只支持 VPC 内云主机资产所绑定公网 IP 的防护。

**Q: 云防火墙互联网边界带宽会限制流量吗？**

A: 云防火墙不会限制流量。

**Q: 业务带宽超峰值带宽限制，会对我有业务影响么？**

A: 如果公网流量大于购买的云防火墙边界带宽，则云防火墙不承诺对超出带宽的流量进行防护。对超出部分的流量，我们会做放行处理。