云防火墙（原生版）

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
04	2025/03/07	主要修改点如下： ● 文档结构调整：区分 C100 实例、N100 实例 ● C100 新增“企业版”相关文档 ● C100 新增“VPC 防护”相关文档 ● C100 新增“日志管理”
03	2024/04/25	主要修改点： ● 新增“批量管理黑白名单规则”和“批量管理防护规则”章节。 ● 新增“地址簿管理”章节。
02	2024/03/12	主要修改点：补充计费说明和最佳实践。
01	2022/11/30	新建文档。

目 录

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。

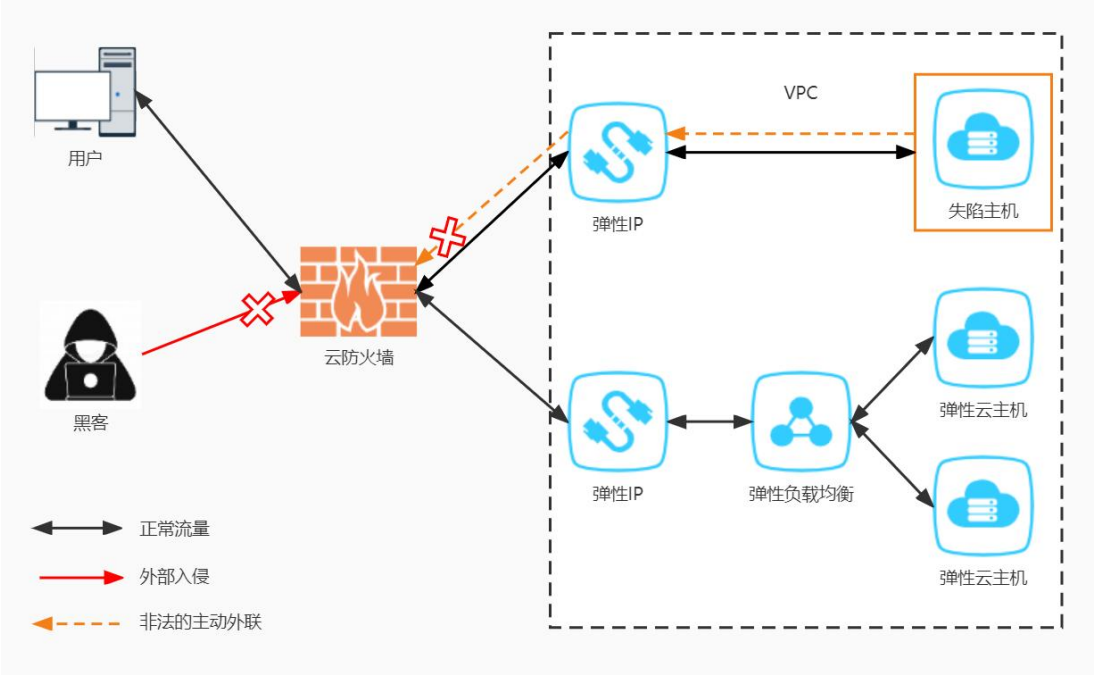
流量可视：提供全面的用户业务流量可视化，实现网络访问可视，网络会话可视，网络行为可视，帮助用户全面感知网络情况。

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好出方向流量趋势。

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. 产品规格

云防火墙（原生版）提供 N100 和 C100 两种类型的实例。

1.6.1. C100 规格

功能		高级版	企业版
互联网边界防火墙	可防护公网 IP 数	高级版套餐默认包含 20 个。 可扩展范围：20 个~1000 个。	企业版套餐默认包含 50 个。 可扩展范围：50 个~1000 个。
	公网流量处理能力	高级版套餐餐默认包含 10Mbps。 可扩展范围：10Mbps~2000Mbps。	企业版套餐默认包含 50Mbps。 可扩展范围：50Mbps~2000Mbps。
VPC 边界防火墙	VPC 边界防火墙配额数	×	企业版套餐默认包含 2 个。 可扩展范围：2 个~150 个。
	VPC 边界流量处理能力	×	企业版套餐默认包含 200Mbps。 可扩展范围：200Mbps~5000Mbps。
网络访问控制		支持策略数 4000	支持策略数 4000
入侵防御检测（IPS）		✓	✓
日志审计		✓	✓
防病毒（Anti-Virus）		×	✓

1.6.2. N100 规格

功能	高级版
防护互联网边界的流量峰值	100Mbps/200Mbps/2Gbps（不可扩展）
防护互联网边界公网 IP 数	20 个（不可扩展）
互联网边界访问控制	支持策略数 4000/6000/20000
VPC 间防火墙	✓
防病毒（Anti-Virus）	✓
入侵防御（IPS）	✓
日志审计	✓

1.7. 产品使用限制

1.7.1. C100 使用限制

- 扩展包上限
  - 防护互联网边界的流量峰值：
    - 高级版：10Mbps~2000Mbps。
    - 企业版：50Mbps~2000Mbps
  - 防护互联网边界公网 IP 数：
    - 高级版：20 个~1000 个。
    - 企业版：50 个~1000 个。
- 访问控制规则上限

  互联网边界防火墙和 VPC 边界防火墙分别支持 4000 条访问控制规则。

1.7.2. N100 使用限制

云防火墙（原生版）- N100 型实例默认不限制日志存储时间；但因本地存储空间有限，云防火墙将在超过存储容量 90%后启动滚动存储策略，增量日志将覆盖历史日志。

如果您有 180 天日志存储的诉求，可参考如下方法进行配置，以确保日志能够被妥善保存：

- 方法一：将日志通过 syslog 外发到专用的日志服务器或者日志审计服务中进行存档与分析（推荐）。
- 方法二：扩容本地磁盘以保证足够的日志存储容量。

1.8. 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	入侵防护

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
		制。	
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-访问控制-中	应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。	云防火墙提供流量记录功能，能够记录所有防火墙的通信会话行为，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。	访问控制
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	应能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	应能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

1.9. 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

类别	云防火墙	Web 应用防火墙
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：

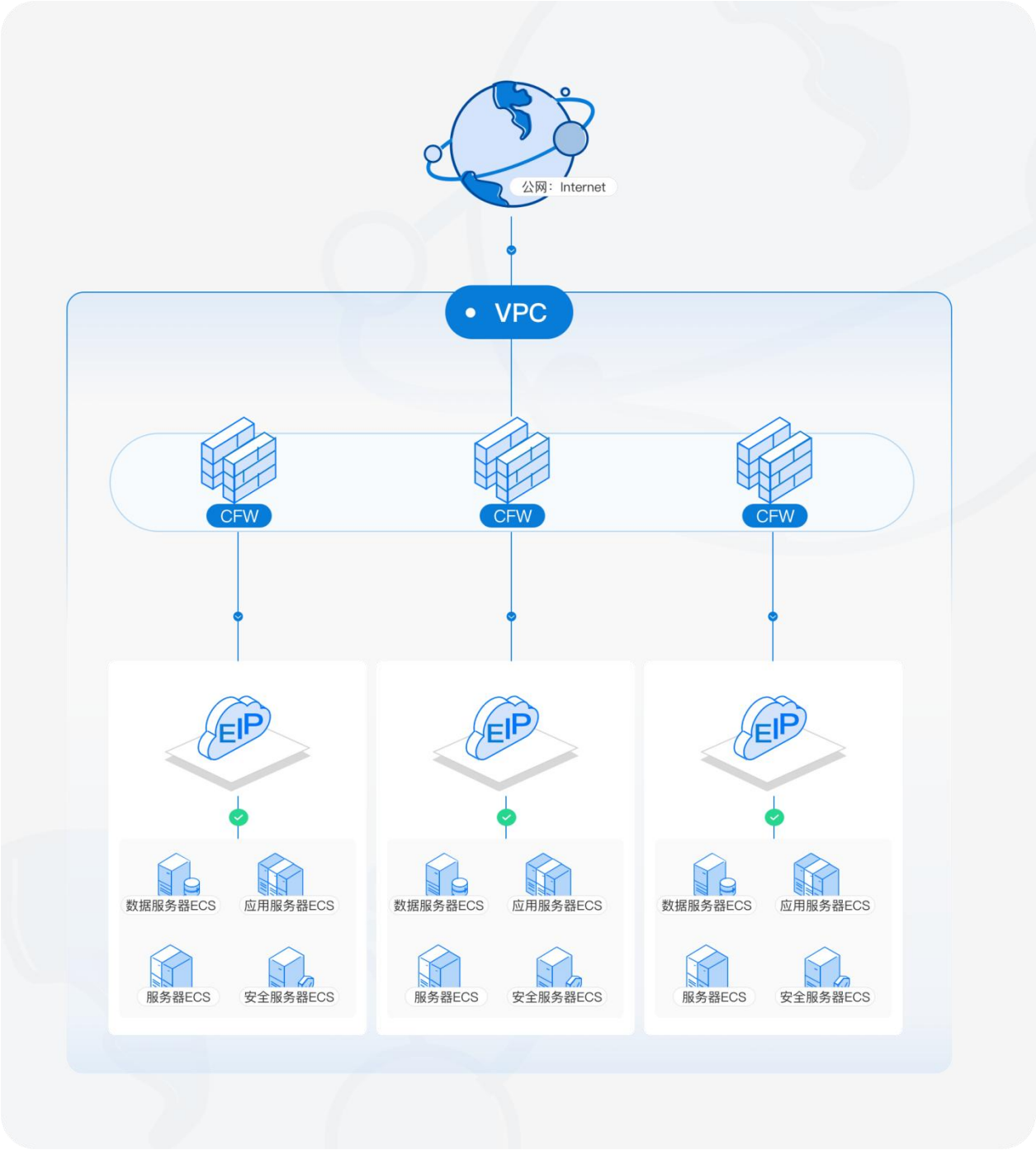
天翼云云防火墙仅能保护部署在天翼云内的弹性云主机网络安全，对于在其他位置的主机和网络设备，因其网络流量未流经天翼云，故天翼云云防火墙无法保护其网络安全。

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，详情请参加弹性 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：


公网：Internet
VPC
CFW
CFW
CFW
EIP
EIP
EIP
数据服务器ECS
应用服务器ECS
服务器ECS
安全服务器ECS
数据服务器ECS
应用服务器ECS
服务器ECS
安全服务器ECS
数据服务器ECS
应用服务器ECS
服务器ECS
安全服务器ECS

1.10. 安全

1.10.1. 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，配置情况等进行审计与监测，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。

1.10.2. 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"
]
}
]
}
```

1.10.3. 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

1.10.4. 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

计费方式

云防火墙（原生版）产品提供**包年包月**计费方式。

N100 标准资费

说明：

- 如下费用仅为 N100 实例的费用。
- 购买云防火墙（原生版）-N100 型实例时，还需要同时购买实例所依赖的基础资源（包括弹性云主机、弹性 IP 等），基础资源与实例一起计费，统一下单。相关基础资源的价格请以对应产品的实际定价为准。

版本	公网流量处理峰值	架构	标准资费（元/月）
高级版	100Mbps	单机	1300
		主备	2300
	200Mbps	单机	2800
		主备	5550
	2Gbps	单机	5600
		主备	11000

C100 标准资费

计费项	高级版资费	企业版资费	计费单位
基础套餐	2800	9600	元/月

计费项	高级版资费	企业版资费	计费单位
公网流量处理能力扩展	50	50	元/Mbps/月
可防护公网 IP 数扩展	50	50	元/个/月
VPC 边界防火墙实例数扩展包	-	2000	元/个/月
VPC 流量处理能力扩展包	-	50	元/10Mbps/月

优惠活动

- 包年订购折扣：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。
- 优惠折扣：云防火墙（原生版）产品订购享受 7 折优惠。该优惠折扣 2025 年 1 月 1 日结束，即在 2025 年 1 月 1 日及之后订购云防火墙（原生版）产品不再享受该优惠折扣。

说明：

- 包年订购折扣与优惠折扣不能同享，取低者计算。
- N100 实例仅支持一次性付费 1 年，不支持一次性付费 2 年、3 年。

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. 续订规则

2.2.1. 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，更多说明见自动续订。

2.2.2. 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将恢复标准价。

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。

2.3. 变配规则

C100 型实例变配规则

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，您可以升级版本或变更配额数量。

- 变更版本：支持从高级版升级到企业版，也支持从企业版降级到高级版。

> 注意：
>
> - 变更版本时，不支持手动对配额数量进行调整。
> - 当未购买扩展包时，才支持将企业版降级到高级版。

- 变更配额数量：您可以对实例的公网流量处理能力、可防护公网 IP 数、VPC 边界防火墙配额数、VPC 边界流量处理能力进行调整，升配和降配均可支持。

  注意：

  - 一次只能变更一种资源的配额数量。
  - 当您进行降配时，降配后的配额不能小于正在防护的资产数。

N100 型实例变配规则

N100 型实例不支持变配。

2.4. 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（包含但不限于规格升级、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. C100 快速入门

3.1.1. 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：

互联网边界防护

操作步骤	说明	相关文档
购买云防火墙（原生版）	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。	购买 C100 实例
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。	● 开启弹性 IP 防护 ● 开启公网 NAT 网关防护
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。 支持配置以下防护策略： ● 入向/出向防护规则：按照 IP 地址、端口、协议、应用等维度设置防护规则进行流量管控。 ● 黑/白名单规则：按照 IP 地址进行流量管控，来自黑名单内的流量会直接拦截，来自白名单内的流量会直接放行。 ● 入侵防御：根据入侵防御规则库拦截网络攻击，支持基础防御、虚拟补丁、DDoS 防护。	● 配置互联网边界防护规则 ● 配置入侵防御防护规则
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。	日志审计

VPC 边界防护

操作步骤	说明	相关文档
购买云防火墙（原生版）	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。	购买 C100 实例
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。	● 开启对等连接防护 ● 开启云专线防护 ● 开启云间高速防护
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。 支持配置以下防护策略： ● 内网互访规则：按照 IP 地址、端口、协议、应用等维度设置防护规则进行流量管控。 ● 黑/白名单规则：按照 IP 地址进行流量管控，来自黑名单内的流量会直接拦截，	● 配置 VPC 边界防护规则 ● 配置入侵防御防护规则

操作步骤	说明	相关文档
	来自白名单内的流量会直接放行。 ● 入侵防御：根据入侵防御规则库拦截网络攻击，支持基础防御、虚拟补丁、DDoS防护。	
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。	日志审计

3.1.2. 购买 C100 实例

前提条件

已注册天翼云账号并完成实名认证。

进入购买页面

方式一：通过产品页进入购买页面

1. 登录天翼云官网。
2. 选择“产品 > 安全及管理 > 网络安全 > 云防火墙（原生版）”，进入云防火墙（原生版）产品详情页面。
3. 单击“立即开通”，进入云防火墙（原生版）订购页面。

方式二：过控制中心进入购买页面

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表中，选择“安全 > 云防火墙（原生版）”，进入云防火墙（原生版）控制台。

购买步骤

1. 进入云防火墙（原生版）订购页面。

2. 配置基本信息。

参数名称	参数说明
区域	选择购买云防火墙（原生版）的区域。
商品类型	此处选择 C100。
版本选择	支持高级版、企业版。

参数名称	参数说明
云防火墙名称	系统会自动为您生成一个名称，您也可以自定义。 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；也可以拖动设置。 ● 高级版可防护公网 IP 数的范围是 20 个 ~ 1000 个。 ● 企业版可防护公网 IP 数的范围是 50 个 ~ 1000 个。 说明： 建议不少于选中 VPC 中防护的公网 IP 数量。
公网流量处理能力	公网流量处理能力是指云防火墙可防护的互联网边界流量峰值。 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；也可以拖动设置。 ● 高级版公网流量处理能力的范围是 10Mbps ~ 2000Mbps。 ● 企业版公网流量处理能力的范围是 50Mbps ~ 2000Mbps。 说明： 建议与您业务的公网带宽保持一致，且不少于选中 VPC 中防护的公网 IP 带宽之和。
VPC 边界防火墙配额数	仅企业版支持 VPC 边界防火墙。 在您的 VPC 下开启每种防护场景将消耗一个配额，已支持的防护场景包括：云专线、云间高速、对等连接等。 可以单击加减号调整 VPC 边界防火墙配额数，步长为 1；也可以在其中直接输入；也可以拖动设置。 VPC 边界防火墙配额数的范围是 2 个 ~ 150 个。
VPC 边界流量处理能力	仅企业版支持 VPC 边界防火墙。 VPC 边界流量处理能力是指可防护的 VPC 边界流量峰值，包含已开启的各类防护场景下的跨 VPC 边界流量之和。 可以单击加减号调整 VPC 边界流量处理能力，步长为 10；也可以在其中直接输入；也可以拖动设置。 VPC 边界流量处理能力的范围是 200Mbps ~ 5000Mbps。

3. 选择“购买时长”，可拖动时间轴设置购买时长。
4. 支持开启“自动续订”，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费。
   - 按月购买，自动续费周期默认为 3 个月。
   - 按年购买，自动续费周期默认为 1 年。

   如需要修改自动续费周期，可进入天翼云“费用中心 > 订单管理 > 续订管理”页面，找到对应的资源进行修改。
5. 参数配置完成后，单击“立即购买”。

6. 确认配置参数和配置费用后，阅读《天翼云云防火墙（原生版）服务协议》，并勾选“我已阅读，理解并同意《天翼云云防火墙（原生版）服务协议》“，点击“立即购买”。

7. 进入“付款”页面，完成付款。

3.2. N100 快速入门

3.2.1. 购买 N100 实例

前提条件

已注册天翼云账号并完成实名认证。

操作步骤

1. 登录天翼云官网。
2. 选择“产品 > 安全及管理 > 网络安全 > 云防火墙（原生版）”，进入云防火墙（原生版）产品详情页面。
3. 单击“立即开通”，进入云防火墙（原生版）订购页面。

4. 配置基本信息。

参数名称	参数说明
区域	选择购买云防火墙（原生版）的区域。
可用区	选择购买云防火墙（原生版）的可用区，默认为随机分配。
商品类型	此处选择 N100。
版本选择	目前仅支持“高级版”。
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。

参数名称	参数说明
云防火墙部署子网	可以下拉选择用户该 VPC 中的子网，展示子网 ID 和子网网段。 需要在防护的 VPC 中创建一个子网掩码不大于 28 的子网网段，在此处选择该子网，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	系统会自动为您生成一个名称，您也可以自定义。 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。
部署架构	支持“单机”和“主备”两种架构。
可防护公网 IP 数	默认为 20 个，不支持修改。
公网流量处理能力	公网流量处理能力是指云防火墙可防护的互联网边界流量峰值，建议与您业务的公网带宽保持一致。 说明： 支持选择 100 Mbps、200 Mbps、2 Gbps，暂不支持扩容。

5. 配置承载云防火墙 N100 实例的云主机规格。

参数	说明
规格	根据所选公网流量处理能力，最低规格要求如下： ● 100 Mbps：规格大于等于 2U4G，基准带宽大于等于 100 Mbps。 ● 200 Mbps：规格大于等于 2U4G，基准带宽大于等于 200 Mbps。 ● 2 Gbps：规格大于等于 4U8G，基准带宽大于等于 2 Gbps。 注意： 如果所选云主机规格低于最低规格要求，则可能会影响云防火墙性能。
购买数量	购买数量根据所选部署架构进行确定，不支持修改。 ● 部署架构选择“单机”时，云主机“购买数量”为 1。 ● 部署架构选择“主备”时，云主机“购买数量”为 2。

6. 为云防火墙 N100 实例的云主机绑定弹性 IP。可以使用已有的弹性 IP，或者单击“购买”，购买新的弹性 IP。

- 部署架构选择“单机”时，只需要 1 个弹性 IP。
- 部署架构选择“主备”时，需要 2 个弹性 IP。

7. 选择“购买时长”，可拖动时间轴设置购买时长。

> 说明：
>
> N100 实例仅支持一次性付费 1 年，不支持一次性付费 2 年、3 年。

8. 支持开启“自动续订”，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费。

- 按月购买，自动续费周期默认为 3 个月。
- 按年购买，自动续费周期默认为 1 年。

如需要修改自动续费周期，可进入天翼云“费用中心 > 订单管理 > 续订管理”页面，找到对应的资源进行修改。

8. 参数配置完成后，单击“立即购买”。

9. 确认配置参数和配置费用后，阅读《天翼云云防火墙（原生版）服务协议》，并勾选“我已阅读，理解并同意《天翼云云防火墙（原生版）服务协议》“，点击“立即购买”。

10. 进入“付款”页面，完成付款。

3.2.2. 登录 N100 实例 Web 页面

前提条件

已购买云防火墙（原生版）N100 型实例。

操作步骤

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航选择“实例监控”，进入云防火墙（原生版）N100 型实例列表页面。

3. 单击目标实例操作列的“配置”，跳转到 N100 型实例的 Web 控制台。

3.3. 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。

C100 型实例实践

实践	描述
云防火墙最佳实践	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

实践	描述
	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。
配置访问控制策略最佳实践	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。

N100 型实例实践

实践	描述
双向访问控制	防火墙作为云计算环境的边界网络安全，符合等级保护要求条例中边界安全访问控制要求项，能够实现内外网访问控制隔离等要求。
SSL VPN 远程拨入	用户存在远程拨入运维请求，但未购买天翼云平台 SSL VPN 服务，可使用防火墙 SSL VPN 服务，该服务需单独配置。

4. 用户指南（C100）

4.1. 购买

4.1.1. 手动续订

约束限制

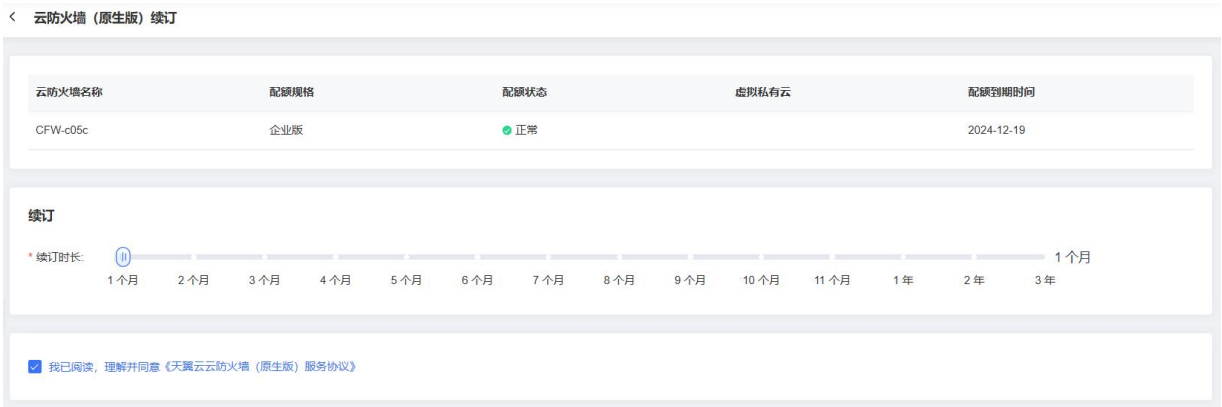
配额状态为“正常”和“已到期”的配额才可以续订。

操作步骤

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 配额管理”，进入配额管理页面。
3. 点击“续订”。

4. 在下图续订页面中，选择续订时长，勾选“我已阅读，理解并同意《天翼云云防火墙（原生版）协议》”后，单击“立即购买”后即可进行续订。

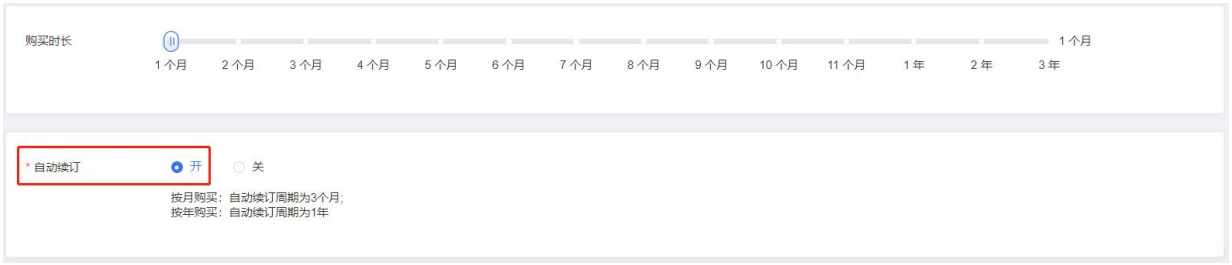
   当续订周期达到 1 年或以上时，订单将可享受包年折扣，续订金额显示折后价。



4.1.2. 自动续订

开通自动续订

- 方法一：云防火墙支持在购买实例时，同步开通“自动续订”。



- 方法二：若开通实例时未开启自动续订，用户也可在开通后，通过天翼云“费用中心 > 订单管理 > 续订管理”页面，开通自动续订。

4.1.3. 变配

云防火墙（原生版）提供“高级版”、“企业版”供用户选择，您可以根据需要，为实例变更版本、为实例变更配额数量。

约束限制

配额状态为“正常”时才支持“变配”。

从高级版升级到企业版

当高级版无法满足您的需求时，你可以升级实例到企业版。

注意：

升级版本时，不支持手动对配额数量进行调整。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 配额管理”，进入配额管理页面。
3. 单击“变配”，进入变配页面。

4. 选择企业版。

5. 确认配置参数和配置费用后，阅读《天翼云云防火墙（原生版）服务协议》，并勾选“我已阅读，理解并同意《天翼云云防火墙（原生版）服务协议》“，点击“立即变配”。
6. 进入“付款”页面，完成付款。

从企业版降级到高级版

当无需 VPC 边界防护时，也可以将实例版本从企业版降级为高级版。

注意：

- 当未购买扩展包时，才支持将企业版降级到高级版。
- 降级版本时，不支持手动对配额数量进行调整。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 配额管理”，进入配额管理页面。
3. 单击“变配”，进入变配页面。
4. 选择高级版。
5. 确认配置参数和可退费用后，阅读《天翼云云防火墙（原生版）服务协议》，并勾选“我已阅读，理解并同意《天翼云云防火墙（原生版）服务协议》“，点击“立即变配”。
6. 进入订单页面，等待订单完成。

变更配额数量

支持对配额数量进行升配、降配。

注意：

- 一次只能变更一种资源的配额数量。
- 当您进行降配时，降配后的配额不能小于正在防护的资产数。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 配额管理”，进入配额管理页面。
3. 单击“变配”，或者单击 VPC 边界防护配额右侧的“扩容”，进入变配页面。

4. 在变配页面，对资源的配额数进行调整。
   - 当前版本为高级版：支持对公网流量处理能力、可防护公网 IP 数进行调整。
   - 当前版本为企业版：支持对公网流量处理能力、可防护公网 IP 数、VPC 边界防火墙配额数、VPC 边界流量处理能力进行调整。

规格	当前版本为高级版	当前版本为企业版
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；也可以拖动设置。 可防护公网 IP 数的范围是 20 个 ~ 1000 个。	
公网流量处理能力	公网流量处理能力是指云防火墙可防护的互联网边界流量峰值。 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；也可以拖动设置。 高级版公网流量处理能力的范围是 10Mbps ~ 2000Mbps。	公网流量处理能力是指云防火墙可防护的互联网边界流量峰值。 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；也可以拖动设置。 企业版公网流量处理能力的范围是 50Mbps ~ 2000Mbps。
VPC 边界防火墙配额数	-	仅企业版支持 VPC 边界防火墙。 在您的 VPC 下开启每种防护场景将消耗一个配额，已支持的防护场景包括：云专线、云间高速、对等连接等。 可以单击加减号调整 VPC 边界防火墙配额数，步长为

规格	当前版本为高级版	当前版本为企业版
		1；也可以在其中直接输入；也可以拖动设置。 VPC 边界防火墙配额数的范围是 2 个 ~ 150 个。
VPC 边界流量处理能力	-	仅企业版支持 VPC 边界防火墙。 VPC 边界流量处理能力是指可防护的 VPC 边界流量峰值，包含已开启的各类防护场景下的跨 VPC 边界流量之和。 可以单击加减号调整 VPC 边界流量处理能力，步长为 10；也可以在其中直接输入；也可以拖动设置。 VPC 边界流量处理能力的范围是 200Mbps ~ 5000Mbps。

5. 确认配置参数和配置费用后，阅读《天翼云云防火墙（原生版）服务协议》，并勾选“我已阅读，理解并同意《天翼云云防火墙（原生版）服务协议》 “，点击“立即变配”。

6. 进入“付款”页面，完成付款。

4.1.4. 退订

若您无需使用云防火墙防护功能时，可以进行退订。当实例中的配额均为“未使用”时才可以执行退订操作。

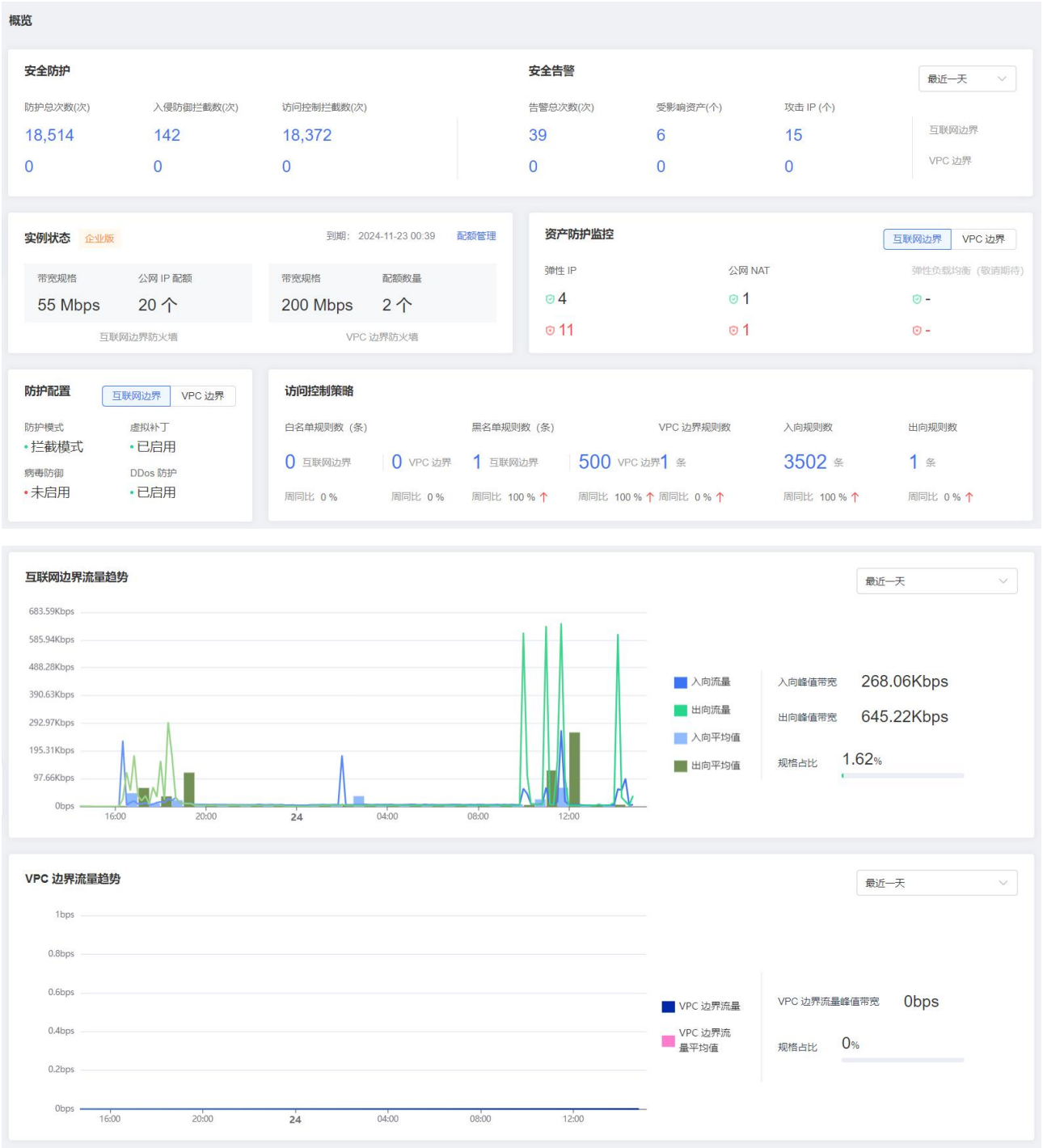
退订步骤

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 配额管理”，进入配额管理页面。
3. 点击“退订”。

4. 在退订页面中，确认退订信息后，勾选“确认退订上述云防火墙（原生版）配额”，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、安全告警、实例状态、资产防护监控、防护配置、访问控制策略、互联网边界流量趋势、VPC 边界流量趋势等统计功能，如下图所示。



安全防护

安全防护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，防护总次数为两项只和。支持查看最近一天、最近三天、最近七天的统计数据。

- 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。点击数字时会跳转至“日志审计 > 入侵防御日志”界面。
- 访问控制拦截数：展示了访问控制拦截的数量。点击数字时会跳转至“日志审计 > 访问控制日志”界面。

安全告警

安全告警展示了告警的总体情况，包括告警总次数、受影响资产、攻击 IP。支持查看最近一天、最近三天、最近七天的统计数据。

- 告警总次数：展示了近期资产触发的告警的总次数。
- 受影响资产：统计存在告警的资产数量。同一资产不重复统计，当同一资产有多个告警时，仅统计一次。
- 攻击 IP：展示了攻击 IP 的数量。同一 IP 不重复统计。
- 点击数字时会跳转至“安全告警”界面。

实例状态

展示实例的版本，互联网边界防火墙实例、VPC 边界防火墙实例的规格和配额。

单击“配额管理”，进入配额管理页面查看更多配额信息。

资产防护监控

资产防护监控展示了防护总体情况，包括已开启和未开启防护的资产数量。

- 绿色图标表示已开启防护的资产数量。
- 红色图标表示未开启防护的资产数量。

防护配置

展示入侵防护策略的配置情况，包括防护模式、虚拟补丁、病毒防御、DDoS 防护。

访问控制策略

展示访问控制策略的配置情况，包括白名单规则数、黑名单规则数、VPC 边界规则数、入向规则数、出向规则数的配置情况及周同比百分比。

- 白名单规则数：分别展示互联网边界和 VPC 边界添加的白名单规则数量，点击数字时会跳转至“访问控制”对应页面。
- 黑名单规则数：分别展示互联网边界和 VPC 边界添加的黑名单规则数量，点击数字时会跳转至“访问控制”对应页面。
- VPC 边界规则数：展示添加的 VPC 边界规则数量，点击数字时会跳转至“访问控制 > VPC 边界规则 > 内网互访规则”页面。
- 入向规则数：展示入向规则数量，点击数字时会跳转至“访问控制 > 互联网边界规则 > 入向规则”页面。
- 出向规则数：展示出向规则数量，点击数字时会跳转至“访问控制 > 互联网边界规则 > 出向规则”页面。

互联网边界流量趋势

展示了近期已开启互联网边界流量防护的资产上的流量趋势。

- 时间范围：可选择最近一天和最近一周。
- 入方向流量：展示了所有开启防护的资产的入流量之和的流量趋势。
- 出方向流量：展示了所有开启防护的资产的出流量之和的流量趋势。
- 入向平均值：展示了所有开启防护的资产的入流量在每个整点的平均值。
- 出向平均值：展示了所有开启防护的资产的出流量在每个整点的平均值。

VPC 边界流量趋势

展示了近期已开启 VPC 边界流量防护的资产上的流量趋势。

- 时间范围：可选择最近一天和最近一周。
- VPC 边界流量：展示了所有开启防护的资产的 VPC 边界流量之和的流量趋势。
- VPC 边界流量平均值：展示了所有开启防护的资产的 VPC 边界流量在每个整点的平均值。

4.3. 防火墙开关

4.3.1. 同步资产

您首次购买后进入云防火墙（原生版）控制台，系统将自动为您同步资产，之后系统默认每天 02:00 自动同步资产信息，你也可以随时手动执行同步资产操作。

手动同步互联网资产

互联网资产包括弹性 IP、公网 NAT 网关。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > 互联网边界防火墙开关”。

3. 单击右上角“同步资产”，系统会立即获取最新的资产信息。

   在资产同步过程中，会显示"资产同步中..."。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。

手动同步 VPC 资产

VPC 资产包括对等连接、云专线、云间高速。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > VPC 边界防火墙开关”。

3. 单击右上角“同步资产”，系统会立即获取最新的资产信息。

   在资产同步过程中，会显示"资产同步中..."。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。

后续操作

同步完成后，资产默认处于关闭防护状态，需要您手动“开启防护”并配置相关的规则。

4.3.2. 互联网边界防火墙

4.3.2.1. 查看互联网边界防护情况

在互联网边界防火墙开关页面上方，用户可以查看互联网边界流量监控信息、防护状态和配额状态。

- 互联网边界流量监控：展示最近 7 天内所有已开启防护资产产生的流量峰值，包括入向峰值带宽和出向峰值带宽；以及当前已购买的带宽规格和带宽占用情况。
- 防护状态：统计了您已开启和未开启防护的弹性 IP、公网 NAT 网关、弹性负载均衡。
- 配额状态：展示已经购买的互联网边界防火墙未使用和已使用的配额数，以及公网 IP 防护配额扩展包的数量。1 个弹性 IP 消耗 1 个防护配额，1 个 NAT 网关消耗 4 个防护配额，1 个弹性负载均衡消耗 1 个防护配额，您可以为 VPC 中的所有弹性 IP、NAT 网关、弹性负载均衡开启防护。

操作步骤

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > 互联网边界防火墙开关”。
3. 查看当前账号下弹性 IP、公网 NAT 网关、弹性负载均衡的防护情况。

4.3.2.2. 开启弹性 IP 防护

注意事项

一个弹性 IP 防护消耗 1 个“可防护公网 IP 数” 配额。

开启弹性 IP 防护

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > 互联网边界防火墙开关”。
3. 在“弹性 IP”页签，找到需要开启防护的弹性 IP，单击操作列的“开启防护”。

   系统会定期自动同步当前账号下的资产到该页面，若有弹性 IP 资产未同步，可以在互联网边界防火墙开关页面右上角单击“同步资产”，手动同步资产。资产同步预计需要 1~2 分钟。

   弹性 IP 列表展示当前账号下所有 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）、私网 IP（实例名称、ID）、虚拟私有云（VPC 名称、VPC 网段）、子网、绑定资产类型、绑定资产（资产名称、ID）、防火墙状态、配额情况。

4. 进入开启弹性 IP 防护页面，完成相应配置。

5. 自动检查：单击“立即扫描”，待扫描完成后，单击“下一步”。

注意：

若有未检查通过的项，请根据提示信息完成相应操作后，再执行下一步。

6. 创建终端节点。

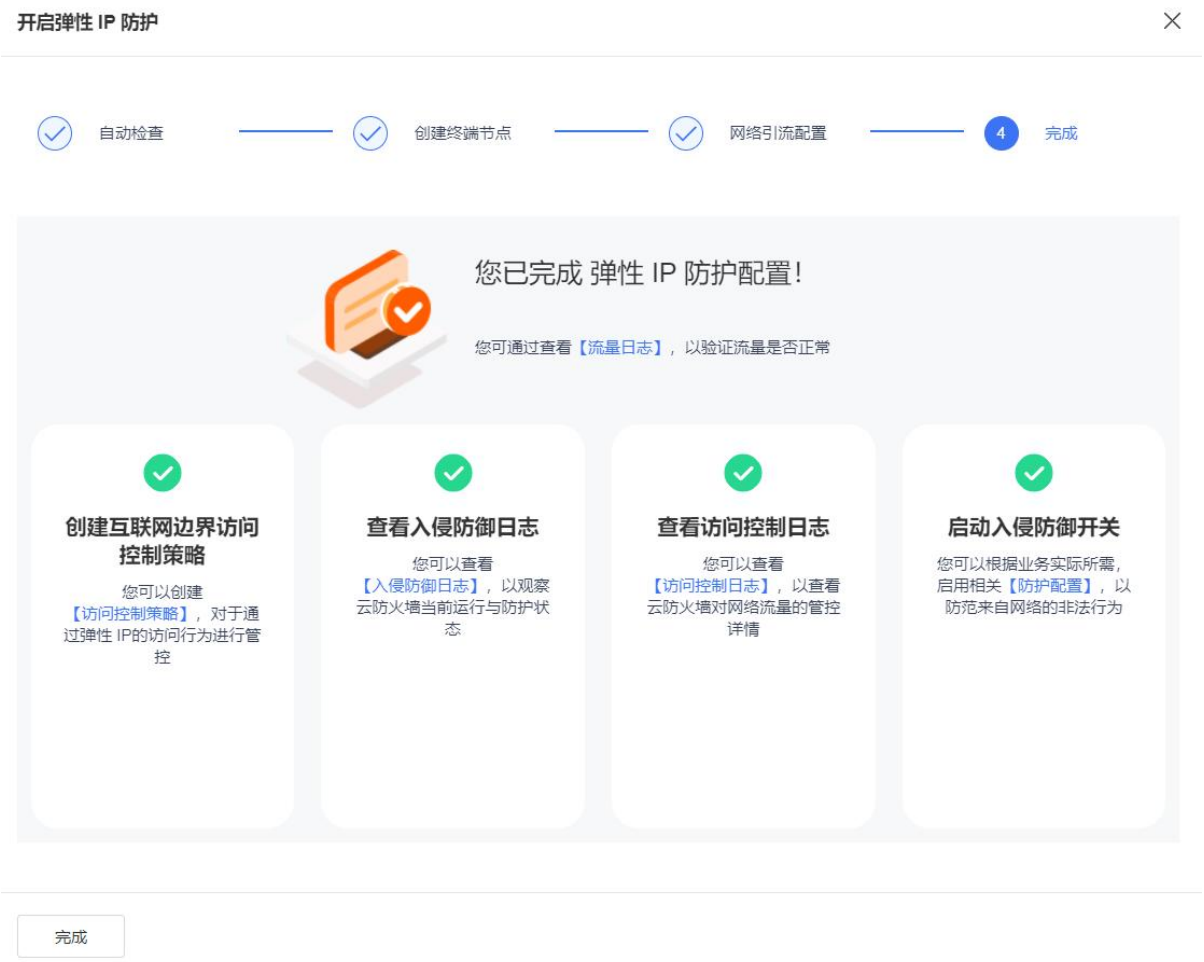
配置引流子网后，单击“创建终端节点”。

注意：

支持选择已有子网，也可以自定义子网。自定义子网的网段必须属于当前 VPC 的 CIDR；创建后无法更改。

终端节点创建完成后，单击“下一步”。

7. 网络引流配置：确认基础信息后，单击“开始引流”。
8. 开启防护成功。



后续操作

开启防护后，您可以为防火墙设置防护策略、查看日志等，以便更好地管控弹性 IP 的流量访问。

- 配置访问控制策略
- 配置入侵防御策略

- 查看访问控制日志
- 查看入侵防御日志
- 查看流量日志

相关操作

关闭防护：若您不需要对弹性 IP 进行防护，可随时关闭防护。

在“弹性 IP”页签，找到需要关闭防护的弹性 IP，单击操作列的“关闭防护”，在弹出的对话框中，单击“确定”为该弹性 IP 关闭防护。

4.3.2.3. 开启公网 NAT 网关防护

前提条件

- 当前账号下已创建公网 NAT 网关。
- 一个公网 NAT 防护将消耗 4 个“可防护公网 IP 数” 配额，在开启防护前，确保有足够的防护配额。

开启公网 NAT 网关防护

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > 互联网边界防火墙开关”。
3. 在“公网 NAT”页签，找到需要开启防护的公网 NAT 网关，单击操作列的“开启防护”。

   系统会定期自动同步当前账号下的资产到该页面，若有公网 NAT 网关资产未同步，可以在互联网边界防火墙开关页面右上角单击“同步资产”，手动同步资产。资产同步预计需要 1~2 分钟。

   公网 NAT 网关列表展示当前账号下所有公网 NAT 网关。列表包括 NAT 名称、NAT 状态、可用区、虚拟私有云、防火墙状态。

4. 进入开启公网 NAT 防护页面，完成相应配置。

5. 自动检查：单击“立即扫描”，待扫描完成后，单击“下一步”。

注意：

若有未检查通过的项，请根据提示信息完成相应操作后，再执行下一步。

6. 创建终端节点。

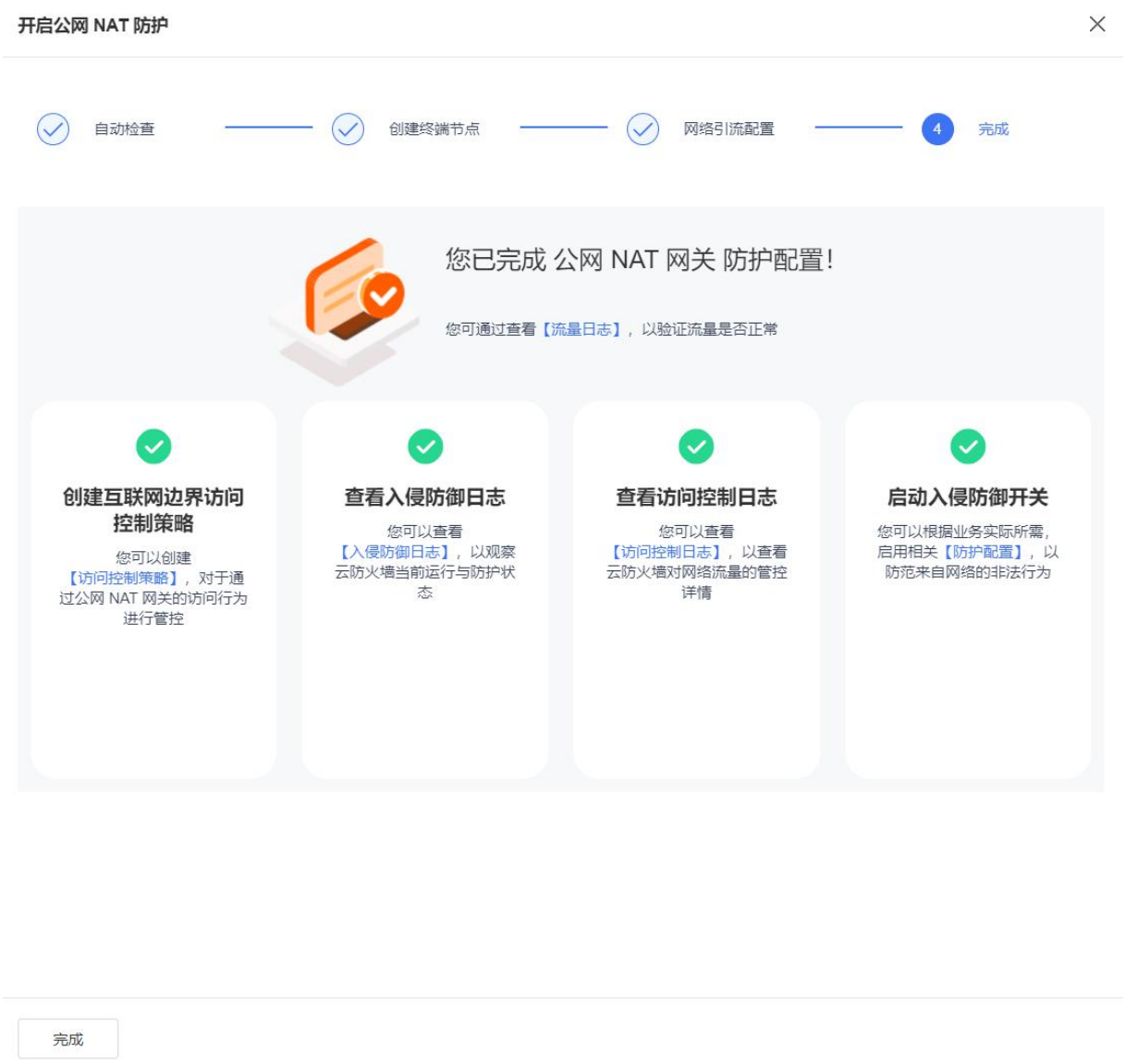
配置引流子网后，单击“创建终端节点”。

注意：

支持选择已有子网，也可以自定义子网。自定义子网的网段必须属于当前 VPC 的 CIDR；创建后无法更改。

终端节点创建完成后，单击“下一步”。

7. 网络引流配置：目前仅支持手动引流，请根据界面提示的步骤完成引流配置。手动配置完成后，单击“配置完成”。
8. 开启防护成功。



后续操作

开启防护后，您可以为防火墙设置防护策略、查看日志等，以便更好地管控公网 NAT 网关的流量访问。

- 配置访问控制策略
- 配置入侵防御策略
- 查看访问控制日志
- 查看入侵防御日志
- 查看流量日志

相关操作

关闭防护：若您不需要对公网 NAT 网关进行防护，可随时关闭防护。

在“公网 NAT”页签，找到需要关闭防护的 NAT 网关，单击操作列的“关闭防护”，在弹出的对话框中，单击“确定”为该 NAT 网关关闭防护。

4.3.2.4. 开启弹性负载均衡防护

注意事项

一个弹性负载均衡防护消耗 1 个“可防护公网 IP 数” 配额。

约束限制

不支持防护“经典型”的负载均衡实例。

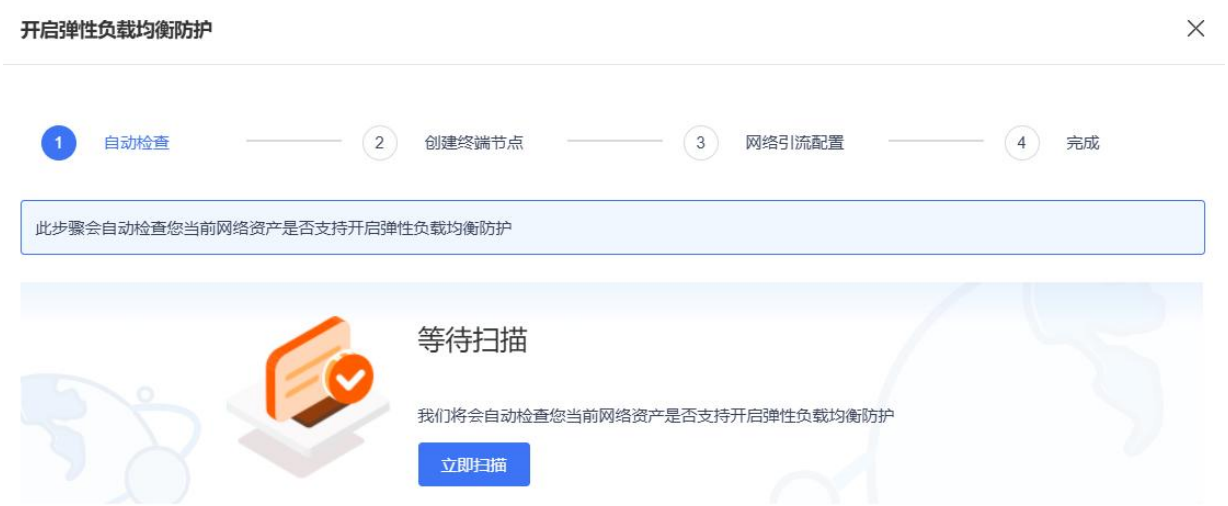
开启弹性负载均衡防护

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > 互联网边界防火墙开关”。
3. 在“弹性负载均衡”页签，找到需要开启防护的弹性负载均衡实例，单击操作列的“开启防护”。

   系统会定期自动同步当前账号下的资产到该页面，若有弹性负载均衡资产未同步，可以在互联网边界防火墙开关页面右上角单击“同步资产”，手动同步资产。资产同步预计需要 1~2 分钟。

弹性负载均衡实例列表展示当前账号下已创建的弹性负载均衡实例。列表包括名称（实例名称）、状态、网络类型、服务地址（包括公网 IP 和内网 IP）、虚拟私有云（VPC 名称、VPC 网段）、子网、IPv4 带宽、防火墙状态。

4. 进入开启弹性负载均衡防护页面，完成相应配置。



5. 自动检查：单击“立即扫描”，待扫描完成后，单击“下一步”。

注意：

若有未检查通过的项，请根据提示信息完成相应操作后，再执行下一步。

6. 创建终端节点。

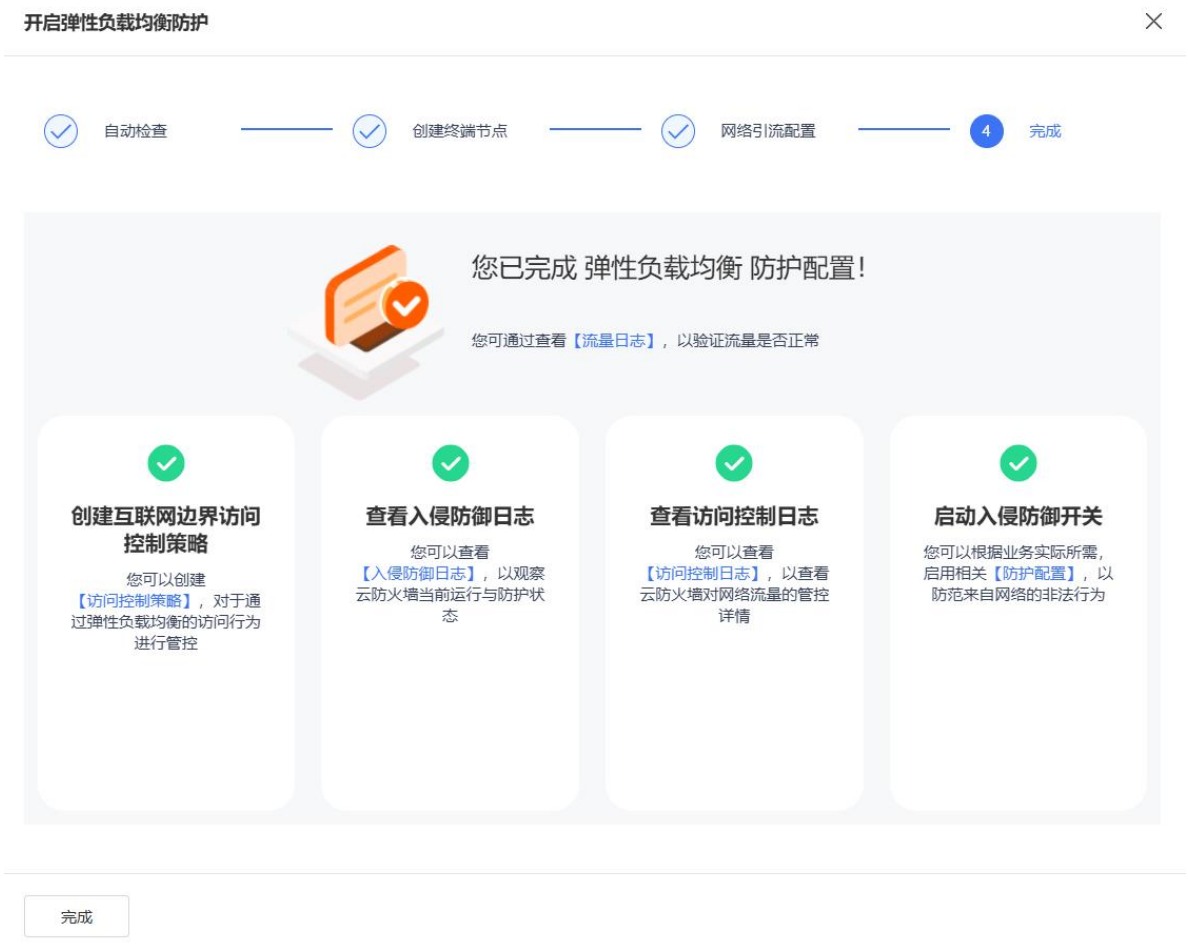
配置引流子网后，单击“创建终端节点”。

注意：

支持选择已有子网，也可以自定义子网。自定义子网的网段必须属于当前 VPC 的 CIDR；创建后无法更改。

终端节点创建完成后，单击“下一步”。

7. 网络引流配置：确认基础信息后，单击“开始引流”。
8. 开启防护成功。



后续操作

开启防护后，您可以为防火墙设置防护策略、查看日志等，以便更好地管控弹性负载均衡的流量访问。

- 配置访问控制策略
- 配置入侵防御策略

- 查看访问控制日志
- 查看入侵防御日志
- 查看流量日志

相关操作

关闭防护：若您不需要对弹性负载均衡进行防护，可随时关闭防护。

注意：

关闭防护前请确保您已提前关闭弹性负载均衡的“VPC 引流开关”，否则可能造成网络中断，影响业务负载。

在“弹性负载均衡”页签，找到需要关闭防护的弹性负载均衡，单击操作列的“关闭防护”，在弹出的对话框中，单击“确定”为该弹性负载均衡关闭防护。

4.3.3. VPC 边界防火墙

4.3.3.1. VPC 边界防火墙概述

VPC 边界防火墙用于防护 VPC 之间的通信流量，VPC 之间通信流量的访问控制，实现内部业务互访活动的可视化与安全防护。

防护对象

- 对等连接
- 云专线
- 云间高速

约束条件

仅“企业版”支持 VPC 边界防火墙。

4.3.3.2. 查看 VPC 边界防护情况

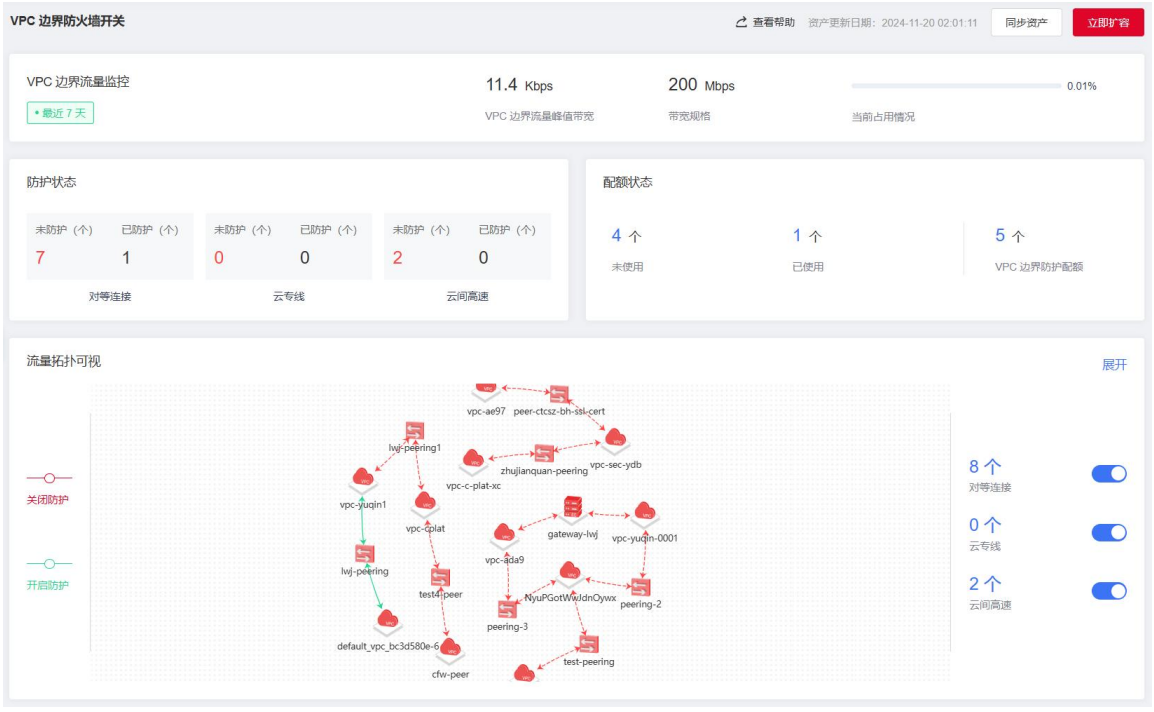
在 VPC 边界防火墙开关页面上方，用户可以查看 VPC 边界流量监控信息、防护状态、配额状态和流量拓扑。

- VPC 边界流量监控：展示最近 7 天内所有已开启防护资产的 VPC 边界流量峰值带宽；以及当前已购买的带宽规格和带宽占用情况。
- 防护状态：统计了您已开启和未开启防护的资产数量，支持防护对等连接、云专线、云间高速资产。

- 配额状态：展示已经购买的 VPC 边界防火墙未使用和已使用的配额数，以及 VPC 边界防护配额总量。1 个防护实例，消耗 1 个防护配额。
- 流量拓扑可视：展示 VPC 边界的网络资产互访关系和防护情况，便于您梳理 VPC 边界访问拓扑并直观掌握整体网络安全防护态势。

操作步骤

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > VPC 边界防火墙开关”。
3. 查看当前账号下对等连接、云专线、云间高速的防护情况。



4.3.3.3. 开启对等连接防护

前提条件

- 当前账号下已创建对等连接。
- 仅“企业版”支持开启对等连接防护。
- 一个对等连接防护将消耗 1 个“VPC 边界防火墙配额数” 配额，在开启防护前，确保有足够的 VPC 边界防护配额。

开启对等连接防护

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > VPC 边界防火墙开关”。
3. 在“对等连接”页签，找到需要开启防护的对等连接实例，单击操作列的“开启防护”。

   系统会定期自动同步当前账号下的资产到该页面，若有对等连接资产未同步，可以在 VPC 边界防火墙开关页面右上角单击“同步资产”，手动同步资产。资产同步预计需要 1~2 分钟。

   对等连接列表展示当前账号下所有对等连接。列表包括名称、状态、连接类型、本端 VPC、本端 VPC 网段、对端 VPC、对端 VPC 网段、防护状态。

4. 进入开启对等连接防护页面，完成相应配置。

5. 自动检查：单击“立即扫描”，待扫描完成后，单击“下一步”。

注意：

若有未检查通过的项，请根据提示信息完成相应操作后，再执行下一步。

6. 创建终端节点。

配置引流子网后，单击“创建终端节点”。

注意：

支持选择已有子网，也可以自定义子网。自定义子网的网段必须属于当前 VPC 的 CIDR；创建后无法更改。

终端节点创建完成后，单击“下一步”。

7. 网络引流配置：目前仅支持手动引流，请根据界面提示的步骤完成引流配置。手动配置完成后，单击“配置完成”。

注意：

若 VPC 下有多个业务子网，每个业务子网须分别进行引流配置。在“本端业务子网”下拉框选择不同业务子网以查看对应配置步骤。

8. 开启防护成功。

后续操作

开启防护后，您可以为防火墙设置防护策略、查看日志等，以便更好地管控对等连接的流量访问。

- 配置访问控制策略
- 配置入侵防御策略
- 查看访问控制日志
- 查看入侵防御日志
- 查看流量日志

相关操作

关闭防护：若您不需要对对等连接进行防护，可随时关闭防护。

注意：

关闭防护前请确保您已提前重置路由表配置，网络流量不再牵引到云防火墙；否则可能造成网络中断，影响业务负载。

在“对等连接”页签，找到需要关闭防护的对等连接，单击操作列的“关闭防护”，在弹出的对话框中，单击“确定”为该对等连接关闭防护。

4.3.3.4. 开启云专线防护

前提条件

- 当前账号下已创建物理专线。
- 仅“企业版”支持开启云专线防护。
- 一个云专线防护将消耗 1 个“VPC 边界防火墙配额数” 配额，在开启防护前，确保有足够的 VPC 边界防护配额。

开启云专线防护

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > VPC 边界防火墙开关”。
3. 在“云专线”页签，找到需要开启防护的云专线实例，单击操作列的“开启防护”。

   系统会定期自动同步当前账号下的资产到该页面，若有云专线资产未同步，可以在 VPC 边界防火墙开关页面右上角单击“同步资产”，手动同步资产。资产同步预计需要 1~2 分钟。

   云专线列表展示当前账号下所有云专线实例。列表包括 VPC 名称、VPC ID、VPC 网段 IPv4、子网网段 IPv4、专线网关名称、专线网关 ID、其他目的网段 IPv4、防护状态。
4. 进入开启云专线防护页面，根据界面提示完成相应配置。

后续操作

开启防护后，您可以为防火墙设置防护策略、查看日志等，以便更好地管控云专线的流量访问。

- 配置访问控制策略
- 配置入侵防御策略
- 查看访问控制日志
- 查看入侵防御日志
- 查看流量日志

相关操作

关闭防护：若您不需要对云专线进行防护，可随时关闭防护。

注意：

关闭防护前请确保您已提前重置路由表配置，网络流量不再牵引到云防火墙；否则可能造成网络中断，影响业务负载。

在“云专线”页签，找到需要关闭防护的云专线资源，单击操作列的“关闭防护”，在弹出的对话框中，单击“确定”为该云专线关闭防护。

4.3.3.5. 开启云间高速防护

前提条件

- 当前账号下已创建云间高速实例，详细操作请参见创建并配置云间高速实例。
- 仅“企业版”支持开启云间高速防护。
- 一个云间高速防护将消耗 1 个“VPC 边界防火墙配额”，在开启防护前，需确保有足够的 VPC 边界防护配额。

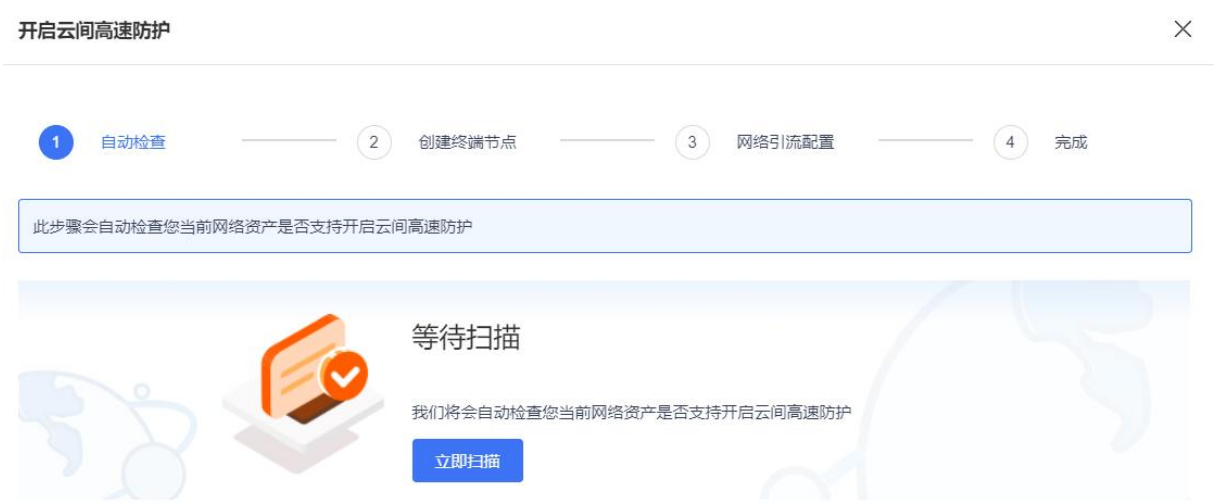
开启云间高速防护

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“防火墙开关 > VPC 边界防火墙开关”。
3. 在“云间高速”页签，找到需要开启防护的 VPC，单击操作列的“开启防护”。

   系统会定期自动同步当前账号下的资产到该页面，若有资产未同步，可以在 VPC 边界防火墙开关页面右上角单击“同步资产”，手动同步资产。资产同步预计需要 1~2 分钟。

   云间高速列表展示当前账号下所有已创建的云间高速实例。列表包括 VPC 名称、VPC ID、状态、子网网段 IPV4、云网关 ID、云间高速名称、云间高速 ID、防护状态。

4. 进入开启云间高速防护页面，完成相应配置。



5. 自动检查：单击“立即扫描”，待扫描完成后，单击“下一步”。

注意：

若有未检查通过的项，请根据提示信息完成相应操作后，再执行下一步。

6. 创建终端节点。

配置引流子网后，单击“创建终端节点”。

注意：

支持选择已有子网，也可以自定义子网。自定义子网的网段必须属于当前 VPC 的 CIDR；创建后无法更改。

终端节点创建完成后，单击“下一步”。

7. 网络引流配置：目前仅支持手动引流，请根据界面提示的步骤完成引流配置。手动配置完成后，单击“配置完成”。

注意：

若 VPC 下有多个业务子网，每个业务子网须分别进行引流配置。在“本端业务子网”下拉框选择不同业务子网以查看对应配置步骤。

8. 开启防护成功。

后续操作

开启防护后，您可以为防火墙设置防护策略、查看日志等，以便更好地管控云间高速的流量访问。

- 配置访问控制策略
- 配置入侵防御策略
- 查看访问控制日志
- 查看入侵防御日志
- 查看流量日志

相关操作

关闭防护：若您不需要对云间高速进行防护，可随时关闭防护。

注意：

关闭防护前请确保您已提前重置路由表配置，网络流量不再牵引到云防火墙；否则可能造成网络中断，影响业务负载。

在“云间高速”页签，找到需要关闭防护的云间高速 VPC，单击操作列的“关闭防护”，在弹出的对话框中，单击“确定”为该 VPC 关闭防护。

4.4. 访问控制

4.4.1. 配置互联网边界防护规则

4.4.1.1. 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。

约束限制

最多支持 4000 条访问控制规则。

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、入向规则数、出向规则数、已占用规格数/总规格。

其中，已占用规格数量=入向规则数+出向规则数+黑名单规则数+白名单规则数。

规则类型

互联网边界防火墙支持如下防护规则，可以根据您的需要分别进行配置。

- 黑名单规则
- 白名单规则
- 入向规则
- 出向规则

防护规则优先级

优先级：黑名单规则 > 白名单规则 > 入向规则 > 出向规则

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。

4.4.1.2. 配置入向/出向规则

添加入向/出向规则

1. 登录云防火墙（原生版）控制台。
2. 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。
3. 选择“入向规则”或“出向规则”页签，单击“添加规则”，在弹出的添加规则页面中，填写防护规则信息。

   规则参数说明如下：

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	● 支持输入 IPv4 地址或使用已添加的地址簿： ● 输入 IPv4：使用“/”隔开掩码，例如 192.168.2.0/24，0.0.0.0/0 表示任意地址。 注意： 添加出向规则时，源 IP 地址配置请配置弹性 IP 所绑定的内网 IP，切勿直接配置弹性 IP 地址，否则规则无法正常生效。

参数名称	参数说明
	● 地址簿选择：通过下拉框选择已添加的 IP 地址簿。
源端口	支持输入端口号或使用已添加的地址簿： ● 输入端口：输入单个端口号或连续的端口号，例如 10 或 1-10，0 表示任意端口。 ● 地址簿选择：通过下拉框选择已添加的端口地址簿。
目的 IP 地址	支持输入 IPv4 地址或使用已添加的地址簿： ● 输入 IPv4：使用“/”隔开掩码，如 192.168.2.0/24，0.0.0.0/0 表示任意地址。 注意 添加入向规则时，目的 IP 地址请配置弹性 IP 所绑定的内网 IP，切勿直接配置弹性 IP 地址，否则规则无法正常生效。 ● 地址簿选择：通过下拉框选择已添加的 IP 地址簿。
目的端口	支持输入端口号或使用已添加的地址簿： ● 输入端口：输入单个端口号或连续的端口号，例如 10 或 1-10，0 表示任意端口。 ● 地址簿选择：通过下拉框选择已添加的端口地址簿。
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、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。支持“最前”、“最后”和“移动至选中规则后”，默认为“最后”。 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。
启用状态	在页面右上方选择是否启用该规则，默认为关。 ● 开：表示启用，规则生效。 ● 关：表示关闭，规则不生效。

4. 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，若未超过则生成相应的防护规则。

管理防护规则

- 编辑规则

  单击防护规则列表操作列中的“编辑”，即可编辑规则。所有规则参数均可修改，相关参数说明请参见添加规则。

- 删除规则

  单击防护规则列表操作列中的“删除”，进行确认后删除该规则。

- 设置优先级

  单击防护规则列表操作列中的“设置优先级”，弹出设置优先级对话框。

  优先级可以选择“最前”、“最后”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。

4.4.1.3. 配置黑白名单规则

添加黑白名单规则

1. 登录云防火墙（原生版）控制台。
2. 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。

3. 选择“黑名单规则”或“白名单规则”页签，单击“添加黑名单”或“添加白名单”，在弹出的添加黑白名单页面中，填写规则信息。

   参数说明如下：

参数名称	参数说明
地址方向	可选择“源地址”或“目的地址”。 ● 源地址：访问流量中的发送数据包的 IP 地址。 ● 目的地址：访问流量中的接收数据包的 IP 地址。
名称	自定义规则名称。名称长度不能超过 100 个字符。
IP 地址	支持输入 IPv4 地址或使用已添加的地址簿： ● 输入 IPv4：使用“/”隔开掩码，如 192.168.2.0/24，0.0.0.0/0 表示任意地址。 ● 地址簿选择：通过下拉框选择已添加的 IP 地址簿，添加 IP 地址簿请参见添加 IP 地址簿。
描述	（可选）自定义规则描述。

4. 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，若未超过则生成相应的防护规则。

删除黑白名单

单击黑白名单列表操作中的“删除”，弹出删除确认框，确定后删除该黑白名单规则，若是“取消”则关闭对话框。

4.4.2. 配置 VPC 边界防护规则

4.4.2.1. 配置内网互访规则

添加内网互访规则

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“访问控制 > VPC 边界规则”，进入 VPC 边界规则页面。
3. 选择“内网互访规则”页签，单击“添加规则”，在弹出的添加规则页面中，填写防护规则信息。

规则参数说明如下：

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	支持输入 IPv4 地址或使用已添加的地址簿： ● 输入 IPv4：使用“/”隔开掩码，例如 192.168.2.0/24，0.0.0.0/0 表示任意地址。 ● 地址簿选择：通过下拉框选择已添加的 IP 地址簿。
源端口	支持输入端口号或使用已添加的地址簿： ● 输入端口：输入单个端口号或连续的端口号，例如 10 或 1-10，0 表示任意端口。 ● 地址簿选择：通过下拉框选择已添加的端口地址簿。
目的 IP 地址	支持输入 IPv4 地址或使用已添加的地址簿： ● 输入 IPv4：使用“/”隔开掩码，如 192.168.2.0/24，0.0.0.0/0 表示任意地址。 ● 地址簿选择：通过下拉框选择已添加的 IP 地址簿。
目的端口	支持输入端口号或使用已添加的地址簿： ● 输入端口：输入单个端口号或连续的端口号，例如 10 或 1-10，0 表示任意端口。 ● 地址簿选择：通过下拉框选择已添加的端口地址簿。
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、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。支持“最前”、“最后”和“移动至选中规则后”，默认为“最后”。 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。

参数名称	参数说明
启用状态	在页面右上方选择是否启用该规则，默认为关。 ● 开：表示启用，规则生效。 ● 关：表示关闭，规则不生效。

4. 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，若未超过则生成相应的防护规则。

管理防护规则

- 编辑规则

  单击防护规则列表操作列中的“编辑”，即可编辑规则。所有规则参数均可修改，相关参数说明请参见添加规则。

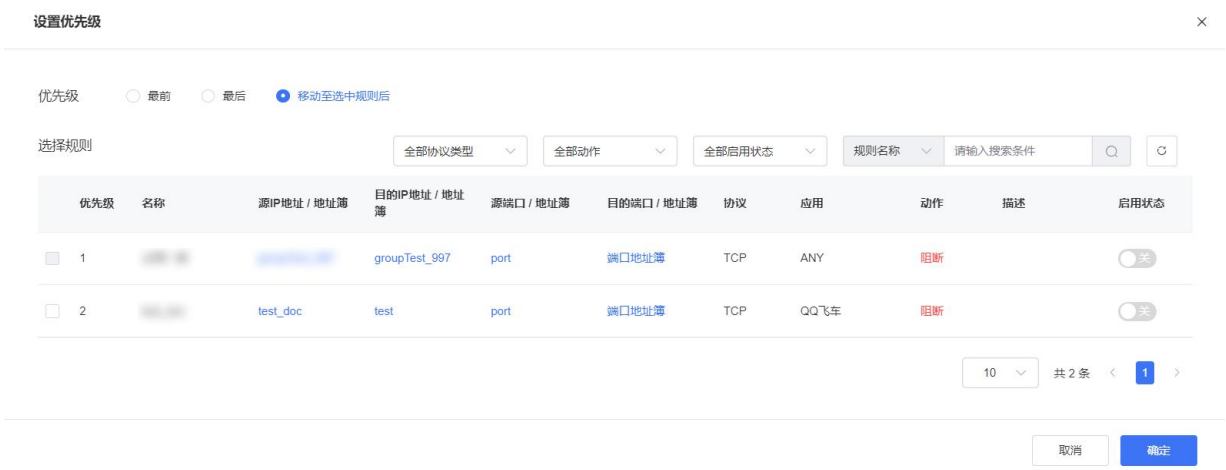
- 删除规则

  单击防护规则列表操作列中的“删除”，进行确认后删除该规则。

- 设置优先级

  单击防护规则列表操作列中的“设置优先级”，弹出设置优先级对话框。

  优先级可以选择“最前”、“最后”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。



4.4.2.2. 配置黑白名单规则

添加黑白名单规则

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“访问控制 > VPC 边界规则”，进入 VPC 边界规则页面。
3. 选择“黑名单规则”或“白名单规则”页签，单击“添加黑名单”或“添加白名单”，在弹出的添加黑白名单页面中，填写规则信息。

   参数说明如下：

参数名称	参数说明
地址方向	可选择“源地址”或“目的地址”。 ● 源地址：访问流量中的发送数据包的 IP 地址。 ● 目的地址：访问流量中的接收数据包的 IP 地址。
名称	自定义规则名称。名称长度不能超过 100 个字符。
IP 地址	支持输入 IPv4 地址或使用已添加的地址簿： ● 输入 IPv4：使用“/”隔开掩码，如 192.168.2.0/24，0.0.0.0/0 表示任意地址。 ● 地址簿选择：通过下拉框选择已添加的 IP 地址簿。
描述	（可选）自定义规则描述。

4. 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，若未超过则生成相应的防护规则。

删除黑白名单

单击黑白名单列表操作中的“删除”，弹出删除确认框，确定后删除该黑白名单规则，若是“取消”则关闭对话框。

4.4.3. 批量管理黑白名单规则

互联网边界防火墙和 VPC 边界防火墙均支持配置黑白名单规则。

下载黑白名单规则模板

1. 登录云防火墙（原生版）控制台。
2. 进入黑白名单规则页面。

   互联网边界：在左侧导航栏选择“访问控制 > 互联网边界规则”，选择“黑名单规则”或者“白名单规则”页签。

   VPC 边界：在左侧导航栏选择“访问控制 > VPC 边界规则”，选择“黑名单规则”或者“白名单规则”页签。
3. 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。
4. 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。

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。

黑白名单规则模板参数说明如下：

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”。 ● 源地址：访问流量中的发送数据包的 IP 地址。 ● 目的地址：访问流量中的接收数据包的 IP 地址。
IP 地址	支持以下格式： ● 地址段，使用“/”隔开掩码，如：192.168.2.0/24 ● IP 地址簿名称。IP 地址簿为多个 IPv4 地址的集合。
描述	自定义规则描述。

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。

4.4.4. 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。

下载防护规则模板

1. 登录云防火墙（原生版）控制台。

2. 进入防护规则页面。

   互联网边界：在左侧导航栏选择“访问控制 > 互联网边界规则”，选择“入向规则”或者“出向规则”页签。

   VPC 边界：在左侧导航栏选择“访问控制 > VPC 边界规则”，选择“内网互访规则”页签。

3. 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。

4. 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。

防护规则参数说明如下：

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： ● 地址段，使用“/”隔开掩码，如：192.168.2.0/24 ● IP 地址簿名称。IP 地址簿为多个 IPv4 地址的集合。
源端口	支持以下格式： ● 端口号。 ● 端口地址簿名称。端口地址簿为多个端口的集合。
目的 IP 地址	支持以下格式： ● 地址段，使用“/”隔开掩码，如：192.168.2.0/24 ● IP 地址簿名称。IP 地址簿为多个 IPv4 地址的集合。
目的端口	支持以下格式： ● 端口号。 ● 端口地址簿名称。端口地址簿为多个端口的集合。
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。

参数名称	参数说明
启用状态	选择该规则是否启用规则。 ● 开：表示启用，规则生效。 ● 关：表示关闭，规则不生效。

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。

4.5. 入侵防御

4.5.1. 防护配置

云防火墙（原生版）的入侵防御功能支持防护网络攻击，可以实时检测并拦截恶意端口扫描、暴力破解、远程代码执行、漏洞利用等云上常见等网络攻击，避免服务器被挖矿或勒索。

防护配置

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“入侵防御 > 防护配置”。
3. 在页面上方切换云防火墙实例。

4. 配置防护模式。
   - 观察模式：针对攻击行为仅记录及告警，不拦截。
   - 拦截模式：自动拦截攻击行为，并记录且告警。

5. 高级设置。

   - 虚拟补丁：针对可被远程利用的高危漏洞，应急漏洞，在网络层提供热补丁，实时拦截漏洞攻击行为，避免修复主机漏洞时对业务产生的中断影响。
   - DDoS 防护：针对常见 DDoS 攻击进行实时自动防御。
   - 病毒防护：通过病毒特征检测来识别病毒文件并产生日志。

4.6. 日志审计

4.6.1. 访问控制日志

约束条件

最多支持查看最近 7 天的日志。

查看日志列表

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 访问控制日志”，进入访问控制日志页面。
3. 在页面上方切换防火墙实例。

4. 查询日志：该列表可根据命中时间、应用、规则名称、协议、判断来源、动作、目的 IP 地址、目的端口、源 IP 地址、源端口、方向进行筛选。

5. 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。

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
2024-10-23 00:22	192.168.2.5	0	8.8.8.8	0	ICMP	--	出向	阻断	8.8.8.8	访问控制	详情
2024-10-23 00:22	192.168.2.5	0	8.8.8.8	0	ICMP	--	出向	阻断	8.8.8.8	访问控制	详情
2024-10-23 00:22	192.168.2.5	0	8.8.8.8	0	ICMP	--	出向	阻断	8.8.8.8	访问控制	详情

查看日志详情

单击操作列的“详情”，可以查看日志命中的规则。

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。

导出日志

> 说明：
>
> 最多支持导出 10000 条数据。

单击“导出”，可以将查询列表中的日志记录导出为 csv 格式。

4.6.2. 入侵防御日志

约束条件

最多支持查看最近 7 天的日志。

查看日志列表

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 入侵防御日志”，进入入侵防御日志页面。
3. 在页面上方切换防火墙实例。

4. 查询日志：该列表可根据命中时间、应用、攻击类型、攻击等级、判断来源、目的 IP 地址、源 IP 地址、方向进行筛选。

5. 入侵防御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、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。

导出日志

> 说明：
>
> 最多支持导出 10000 条数据。

单击“导出”，可以将查询列表中的日志记录导出为 csv 格式。

4.6.3. 流量日志

约束条件

- 最多支持查看最近 7 天的日志。
- 流量日志将在网络会话连接断开后被上报。

查看日志列表

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 流量日志”，进入流量日志页面。
3. 在页面上方切换防火墙实例。

4. 查询日志：该列表可根据命中时间、应用、协议、目的端口、动作、源 IP 地址、源端口、目的 IP 地址、方向进行筛选。

5. 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。

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
2024-10-23 11:38	11.5.0.26	10611	192.168.2.5	0	ICMP	--	入向	放行	28B	1	--
2024-10-23 11:38	11.5.0.26	10610	192.168.2.5	0	ICMP	--	入向	放行	28B	1	--
2024-10-23 11:38	11.5.0.26	4585	192.168.2.4	0	ICMP	--	入向	放行	28B	1	--

流量日志参数说明

参数	说明
发生时间	流量日志上报的时间。
源 IP 地址	该条流量的源 IP 地址。
源端口	该条流量的源端口。
目的 IP 地址	访问的目的 IP。
目的端口	该条流量的目的端口。
协议	该条流量的协议类型。
应用	该条流量所属应用。
方向	该条流量会话是入方向或是出方向。仅互联网边界防火墙有该参数。
动作	该条流量被拦截或放行。
流字节数	防护流量的字节总数。
流报文数	防护流量的报文总数。
规则名	该条流量匹配到的防护规则名称。

导出日志

说明：

最多支持导出 10000 条数据。

单击“导出”，可以将查询列表中的日志记录导出为 csv 格式。

4.6.4. 病毒防护日志

约束条件

最多支持查看最近 7 天的日志。

查看日志列表

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 病毒防护日志”，进入病毒防护日志页面。
3. 在页面上方切换防火墙实例。

4. 查询日志：该列表可根据命中时间、应用、病毒名称、协议、MD5、动作、目的端口、目的 IP 地址、源端口、源 IP 地址进行筛选。

5. 病毒防护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、动作、病毒名称、MD5。

导出日志

说明：

最多支持导出 10000 条数据。

单击“导出”，可以将查询列表中的日志记录导出为 csv 格式。

4.6.5. 操作日志

约束条件

最多支持查看最近 7 天的日志。

查看日志列表

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 操作日志”，进入操作日志页面。
3. 在页面上方切换防火墙实例。

4. 查询日志：该列表可根据命中时间、危险等级、操作行为、日志内容进行筛选。

5. 操作日志列表包括发生时间、危险等级、操作行为、日志内容。

导出日志

说明：

最多支持导出 10000 条数据。

单击“导出”，可以将查询列表中的日志记录导出为 csv 格式。

4.6.6. 日志管理

云防火墙（原生版）支持存储访问控制日志、入侵防御日志、流量日志、病毒防护日志、操作日志，日志存储容量默认为 50G，日志存储时长默认为 7 天。

当默认的日志配置无法满足您的业务需求时：

- 您可以根据业务需求对日志存储类型、日志存储时长进行调整，具体操作请参见配置日志存储类型、修改日志存储时长。
- 对于需要长期存储的日志数据，您可以创建日志投递任务，将日志归档至对象存储服务中长期保存。

查看日志存储容量

日志存储容量默认为 50G，存储容量达到上限后，将滚动清理超限日志，请定期关注日志存储容量的使用情况。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 日志管理”，进入日志管理页面。
3. 在页面上方切换防火墙实例。
4. 在存储容量模块可查看存储容量、存储使用量。

配置日志存储类型

云防火墙（原生版）支持访问控制日志、入侵防御日志、流量日志、病毒防护日志、操作日志。

说明：

- 操作日志必须勾选，其他类型的日志可以根据实际情况进行选择。
- 若去勾选某中类型的日志，云防火墙（原生版）不会删除已存储的日志，但不会再继续存储新的日志。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 日志管理”，进入日志管理页面。
3. 在页面上方切换防火墙实例。
4. 在日志存储类型模块单击“点击修改”。

5. 在弹出的对话框中，选择日志存储类型。

6. 选择完成后，单击“确定”。

修改日志存储时长

日志存储时长默认为 7 天，您可以根据实际情况修改日志存储时长，日志存储时长支持 7~365 天。

注意：

日志存储容量达到上限后，将滚动清理超限日志，届时将无法保证存储时长。对于需要长期存储的日志数据，您可以创建日志投递任务，将日志归档至对象存储服务中长期保存。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 日志管理”，进入日志管理页面。
3. 在页面上方切换防火墙实例。
4. 在日志存储时长模块单击“点击修改”。

5. 在弹出的对话框中，配置日志存储时长。

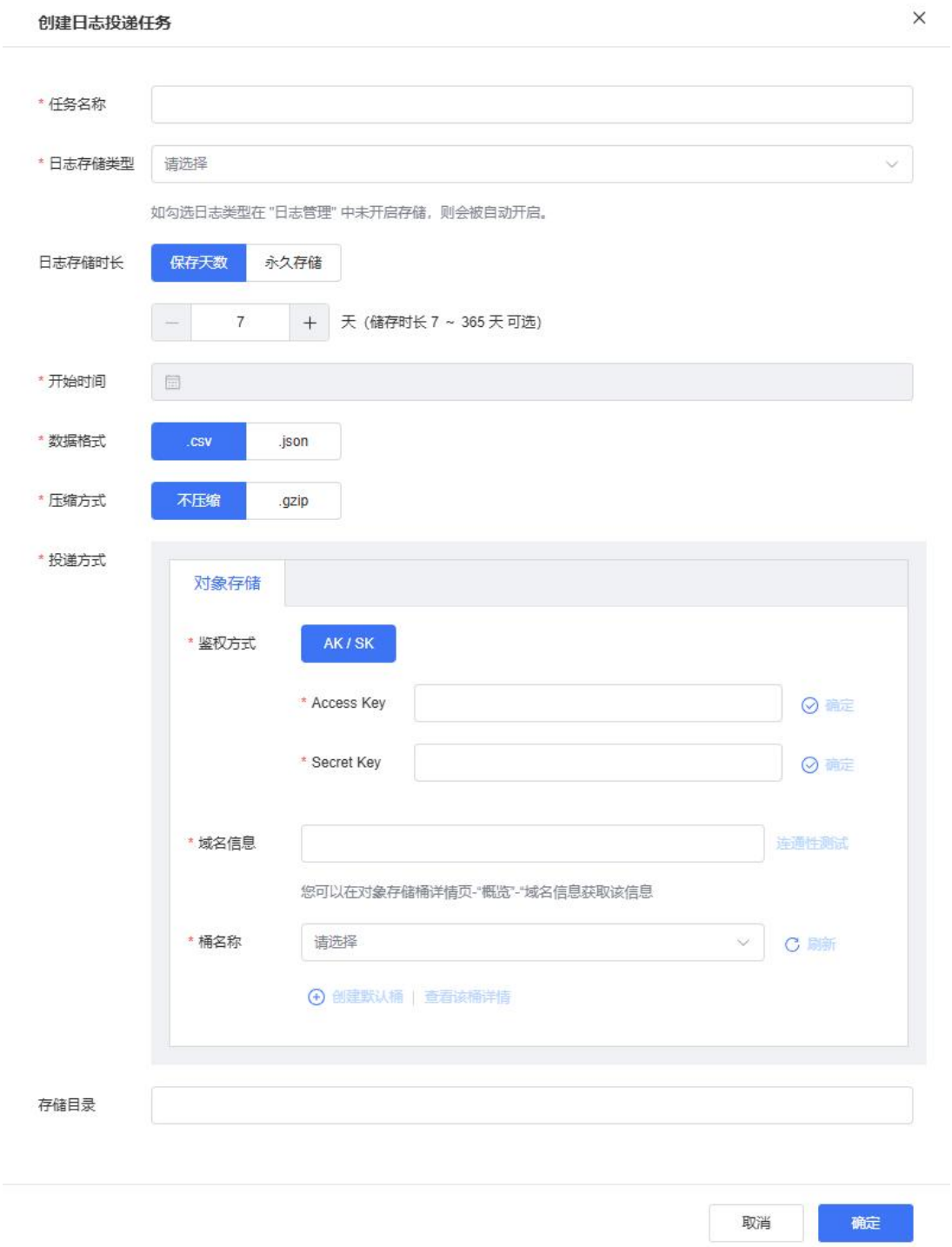
6. 配置完成后，单击“确定”。

创建日志投递任务

您可以将访问控制日志、入侵防御日志、流量日志、病毒防护日志投递到对象存储服务进行存储。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“日志审计 > 日志管理”，进入日志管理页面。
3. 在页面上方切换防火墙实例。

4. 单击“创建日志投递任务”，弹出创建日志投递任务窗口。



5. 配置日志投递任务参数。

参数	说明

参数	说明
任务名称	自定义任务名称。
日志存储类型	选择需要投递到对象存储的日志类型，若日志管理中未开启存储，将会被自动开启。
日志存储时长	支持永久存储，或自定义日志存储时长（7~365 天）。
开始时间	日志开始投递到对象存储的时间。
数据格式	支持将日志存储为“.csv”和“.json”格式。
压缩方式	支持压缩为“.gzip”格式，或者不压缩日志文件。
投递方式	目前支持“对象存储”方式，将日志投递到对象存储桶中进行存储。 ● 鉴权方式：通过对象存储 AK/SK 进行鉴权。配置 AK/SK 后，单击右侧“确定”。 ● 域名信息：域名信息配置后，单击右侧“连通性测试”测试云防火墙与对象存储的连通性。 ● 桶名称：通过下拉列表选择桶。
存储目录	配置日志在桶中存储的目录。 ● 若不配置，则存储在桶的根目录。 ● 若配置的目录在桶中不存在，则自动在桶中创建对应的目录。

6. 配置完成后，单击“确定”。回到日志管理页面，在任务列表可查看已创建的任务。

相关操作：

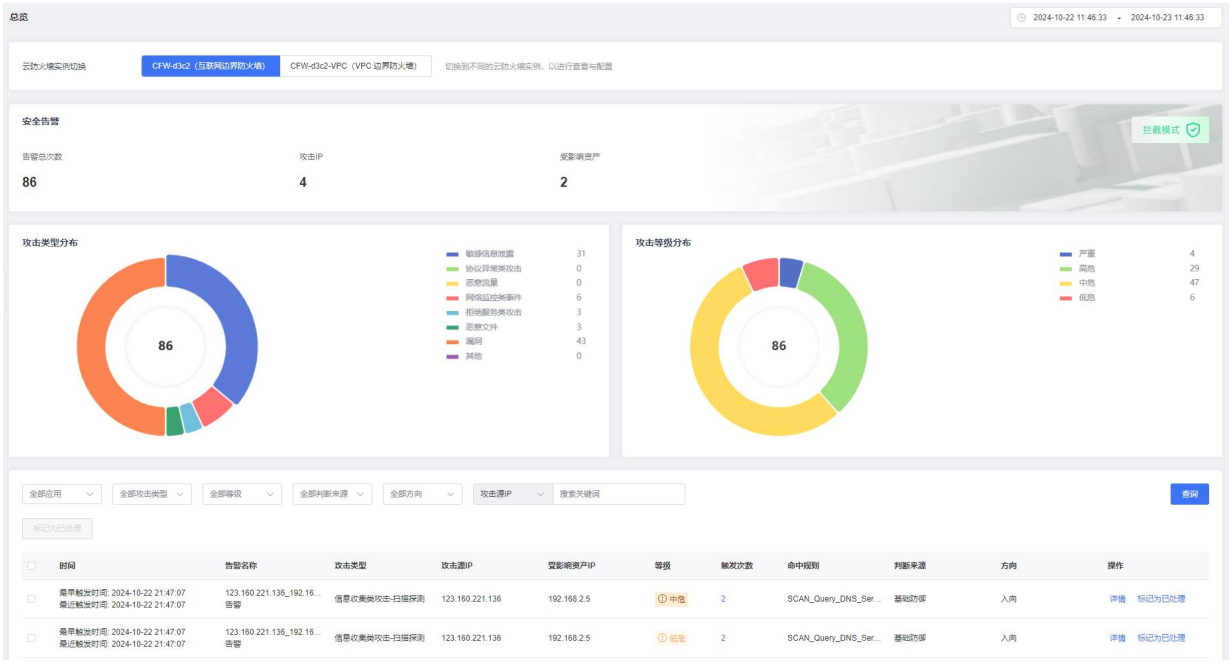
- 投递状态变更：可随时对日志投递任务进行开启或关闭。
- 编辑日志投递任务：支持修改日志存储时长、数据格式、压缩方式、投递方式、存储目录。
- 删除投递任务：若不需要某个投递任务时，可以删除投递任务。

4.7. 安全告警

查看告警列表

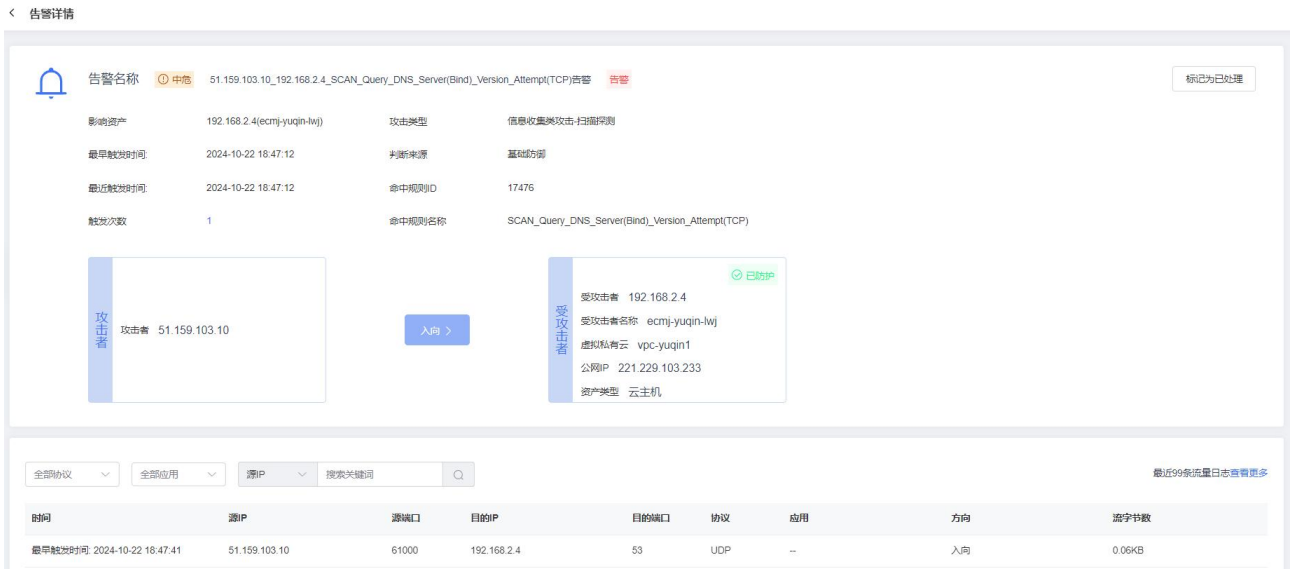
1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“安全告警”，进入安全告警页面。
3. 在页面上方切换防火墙实例。

> 说明：
>
> 默认展示近一天的告警，可在页面右上角自定义查看的时间范围。



查看告警详情

单击告警列表操作列的“详情”，进入告警详情页面。在该页面可以查看告警的详细信息。



处理告警

若您已手动处理告警，可将其“标记为已处理”，标记后，告警的状态将从“未处理”变为“已处理”。

操作步骤：单击“标记为已处理”，在弹出的确认框中，单击“确定”。

4.8. 设置中心

4.8.1. 配额管理

配额管理页面最上方为您提供了云防火墙（原生版）配额订购入口，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信息。

查看配额

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 > 配额管理”，进入“配额管理”页面。

- 配额展示信息包括配额的状态、资源 ID、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。
- 支持对配额进行续订、变配。
- 支持修改防火墙名称。

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。

续订

配额状态为“正常”时才可以执行续订操作。

变配

配额状态为“正常”时才可以执行变配操作。

退订

若您无需使用云防火墙防护功能时，可以进行退订。当实例中的配额均为“未使用”时才可以执行退订操作。


正常 | CFW-d3c2 | 企业版
续订 | 变配 | 退订 | 编辑
资源 ID ffa04ae945d948ad914015b218990d0e
可防护/已防护公网 IP 数 20 / 0 个
公网流量处理能力 55Mbps
配额订购时间 2024-10-23
配额到期时间 2024-11-23
实例 ID CFW-d3c2-VPC
实例类型 VPC 边界防火墙
VPC 边界防护配额 0 / 2 + 扩容
VPC 边界流量峰值带宽 200Mbps 查看流量监控 + 扩容

4.8.2. 报表管理

云防火墙（原生版）支持对互联网边界防火墙和 VPC 边界防火墙生成防护报表，包括日报、周报、月报，并支持订阅报表，订阅后系统会在报表生成后将报表发送至您的邮箱。

前提条件

- 已购买云防火墙（原生版）C100 型实例。
- 已开启防护。

配置报表

报表配置全局生效，即对互联网边界防火墙和 VPC 边界防火墙实例均生效。

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 报表管理”，进入报表管理页面。
3. 在“报表管理”页面右上角，单击“报表配置”，进入报表配置页面。

配置如下参数：

参数名称	说明

参数名称	说明
报表生成	支持生成日报、周报、月报。根据需要进行开启，可多选。 ● 日报：每天 00:00:00 生成前一日的报表。 ● 周报：每周一 00:00:00 生成前一周的报表。 ● 月报：每月 1 日 00:00:00 生成前一月的报表。
报表订阅	该页面自动列出当前账号及其全部子账号。 勾选需要订阅报表的账号，报表生成后，系统会自动发送报表至订阅账号的邮箱。

4. 单击“确认”，完成报表配置。

查看及下载报表

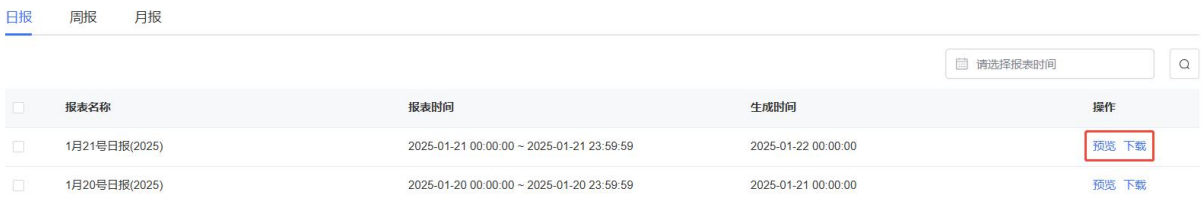
报表保留周期如下表所示，建议您定期下载报表，以满足等保测评以及审计的需要。

报表类型	保留周期
日报	报表保存 180 天，约半年
周报	报表保存 52 周，约一年
月报	报表保存 24 个月，约两年

请参考如下步骤查看及下载报表：

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 报表管理”，进入报表管理页面。
3. 在页面上方切换防火墙实例。

4. 在目标报表所在行的“操作”列，单击“预览”即可查看报表内容，单击“下载”即可将报表下载到本地。



4.8.3. 通知设置

在通知设置页面，您可以开启入侵检测告警通知，配置接收告警通知的接收人等。

开启/关闭告警通知

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 通知设置”，进入通知设置页面。
3. 生效状态为“开”表示已开启告警通知；“关”表示已关闭告警通知。

配置告警通知

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航栏，选择“设置中心 > 通知设置”，进入通知设置页面。

3. 单击通知项操作列的“编辑”，进入通知项配置页面。

4. 配置通知类型、通知时间和消息接收人。

参数名称	说明
通知类型	支持严重、高危、中危、低危。
通知时间	全天、时段（8:00-20:00）
消息接收人	该页面自动列出当前账号及其全部子账号。 勾选需要接收告警通知的账号，当有告警时，系统会自动发送告警信息至所选账号的邮箱。

5. 配置告警通知开关。

   生效状态为“开”表示开启告警通知；“关”表示关闭告警通知。

6. 配置完成后，单击“确定”，保存配置。

4.8.4. 地址簿管理

4.8.4.1. 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. 单击“添加地址簿”，进入“地址簿添加”页面。

6. 配置地址簿参数，参数说明如下。

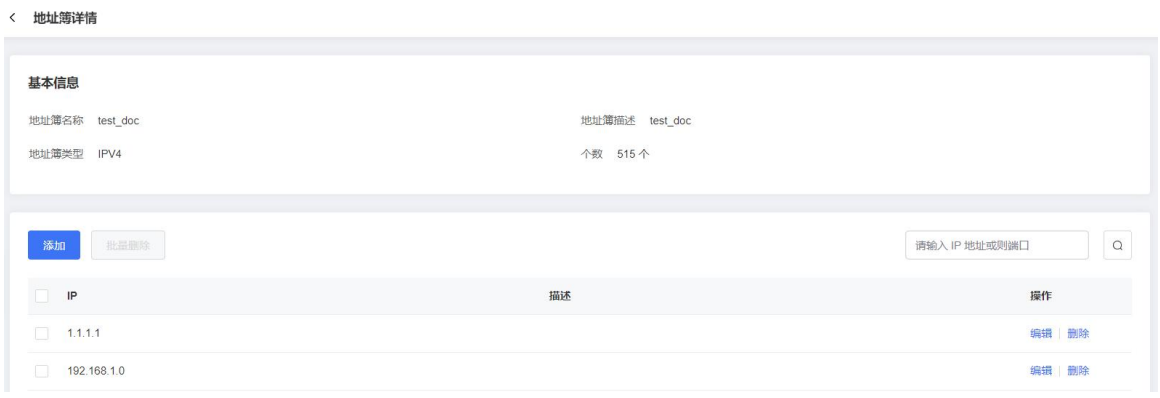
参数名称	参数说明
地址簿名称	用户可自定义地址簿名称。 命名规则如下： 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_）。 长度不超过 255 字符。
地址簿类型	IP 地址簿选择“IPv4 地址”。
地址簿描述	用于标识地址簿的用途，以便快速区分不同的地址簿。

参数名称	参数说明
IP 地址	添加该 IP 地址簿需要管理的 IP 地址。最多支持 1000 个地址。 支持如下地址格式： ● 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。

7. 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. 找到目标地址簿，单击目标地址簿操作列的“详情”。
6. 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. 找到需要删除的地址簿，单击目标地址簿操作列的“删除”。
6. 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：

- 配置互联网边界防护规则：
  - 配置入向/出向规则
  - 配置黑白名单规则
- 配置 VPC 边界防护规则：
  - 配置内网互访规则
  - 配置黑白名单规则

4.8.4.2. 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. 单击“添加地址簿”，进入“地址簿添加”页面。

6. 配置地址簿参数，参数说明如下。

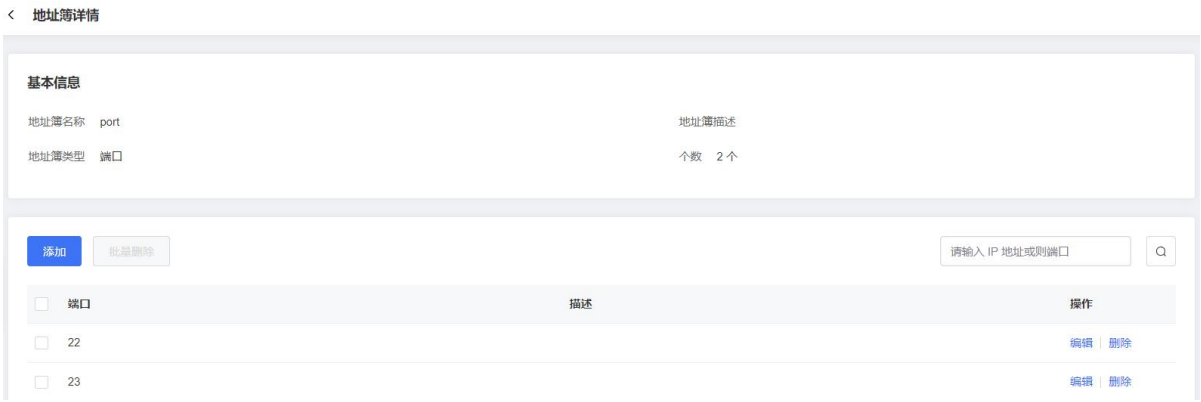
参数名称	参数说明
地址簿名称	用户可自定义地址簿名称。 命名规则如下： ● 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_）。 ● 长度不超过 255 字符。
地址簿类型	端口地址簿选择“端口”。

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	添加该端口地址簿需要管理的端口。最多支持 50 个端口。 支持如下格式： ● 单个端口，如：80。 ● 多个连续端口，中间使用“-”隔开，如：80-443。 ● 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。

7. 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. 找到目标地址簿，单击目标地址簿操作列的“详情”。
6. 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. 找到需要删除的地址簿，单击目标地址簿操作列的“删除”。
6. 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：

- 配置互联网边界防护规则：配置入向/出向规则
- 配置 VPC 边界防护规则：配置内网互访规则

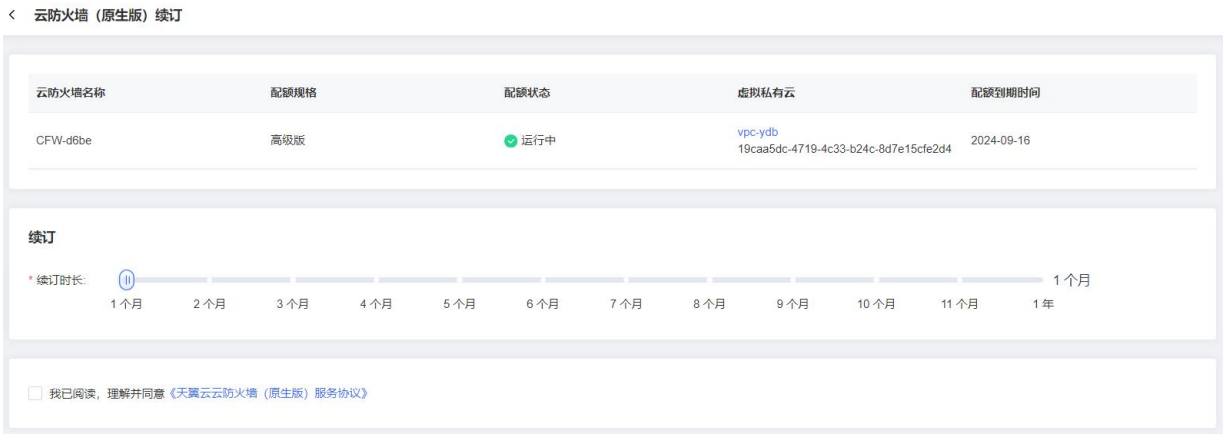
5. 用户指南（N100）

5.1. 购买相关

5.1.1. 续订

1. 购买 N100 实例后，默认进入云防火墙（原生版）N100 实例监控页面。

2. 单击实例列表操作列的“续订”，进入续订页面。



3. 选择“续订时长”。
4. 阅读《天翼云云防火墙（原生版）服务协议》并勾选“我已阅读，理解并同意《天翼云云防火墙（原生版）服务协议》”，单击“立即购买”。
5. 进入付款页面，完成付款。

5.1.2. 退订

支持在费用中心“退订管理”页面退订云防火墙（原生版）N100 型实例。退订实例时，还需要同步退订相应的云主机资源。

退订步骤

1. 进入云防火墙（原生版）控制台，在 N100 型实例页面，获取要退订资源的资源 ID、弹性 IP。

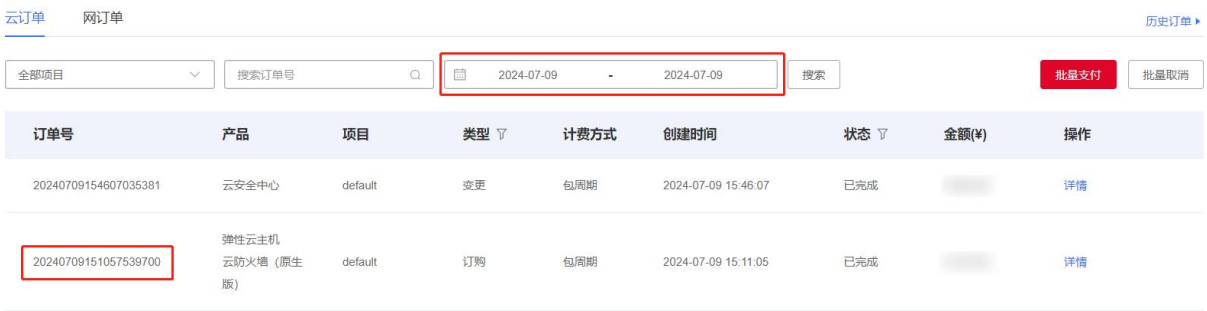
2. 进入弹性云主机控制台，根据弹性 IP 找到相应的云主机，并将云主机关机。

注意：

若不关机，会导致云主机资源退订不成功。

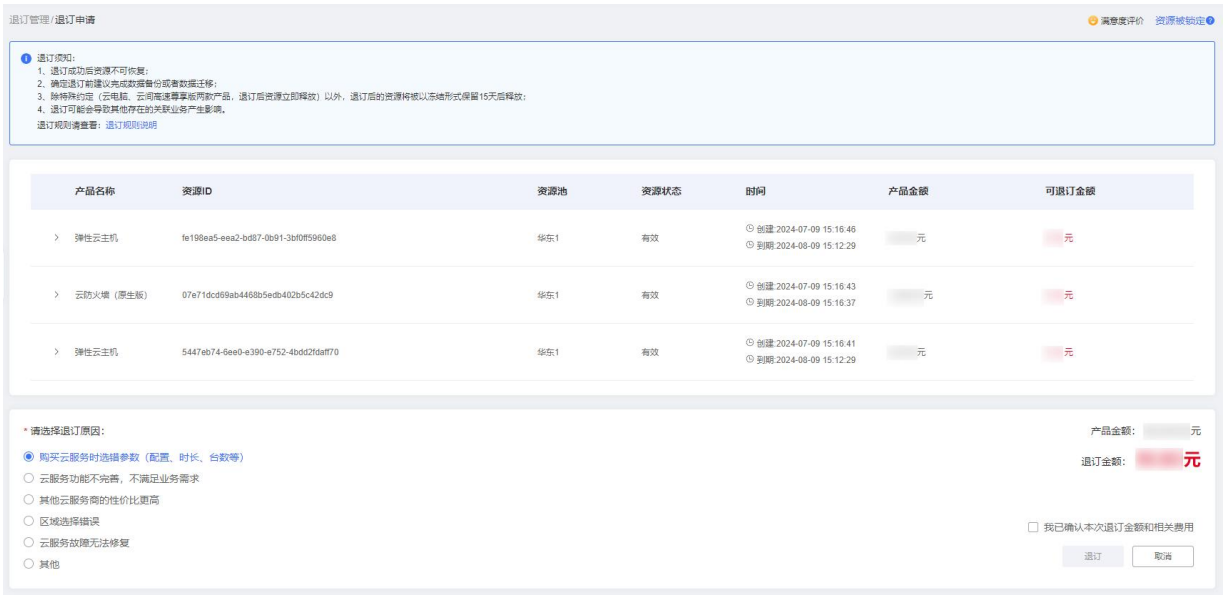
3. 进入“费用中心 > 订单管理 > 退订管理”页面，搜索“云防火墙（原生版）防护”，在查找出的资源列表中，根据资源 ID 找到要退订的订单号。

或者在“费用中心 > 订单管理 > 我的订单”页面，根据资源创建日期等信息，查找需要退订的订单号。



4. 在“费用中心 > 订单管理 > 退订管理”页面页面，根据订单号，查找需要退订的资源。

5. 勾选复选框，单击列表上方的“批量退订”，或单击操作列的“退订”，依次退订云防火墙（原生版）资源和相应的云主机资源。
6. 在弹出的退订申请页面，确认退订信息、退订金额，选择退订原因，勾选“我已确认本次退订金额和相关费用”，单击“退订”。



7. 退订申请提交成功后，您可以进入“费用中心 > 订单管理 > 我的订单”页面，在订单详情中查看退订进度。

一共会生成三个退订订单，当退订订单状态均为“退订完成”时，表示退订成功。

5.2. 使用相关

前提条件

已购买云防火墙（原生版）N100 型实例。

登录 N100 实例控制台

1. 登录云防火墙（原生版）控制台。
2. 在左侧导航选择“实例监控”或“云防火墙 - N100 型”，进入云防火墙（原生版）N100 型实例列表页面。
3. 单击目标实例操作列的“配置”，跳转到 N100 实例的控制台，默认进入控制台首页。

使用 N100 实例

请参见《云防火墙（原生版）N100 用户指南》。

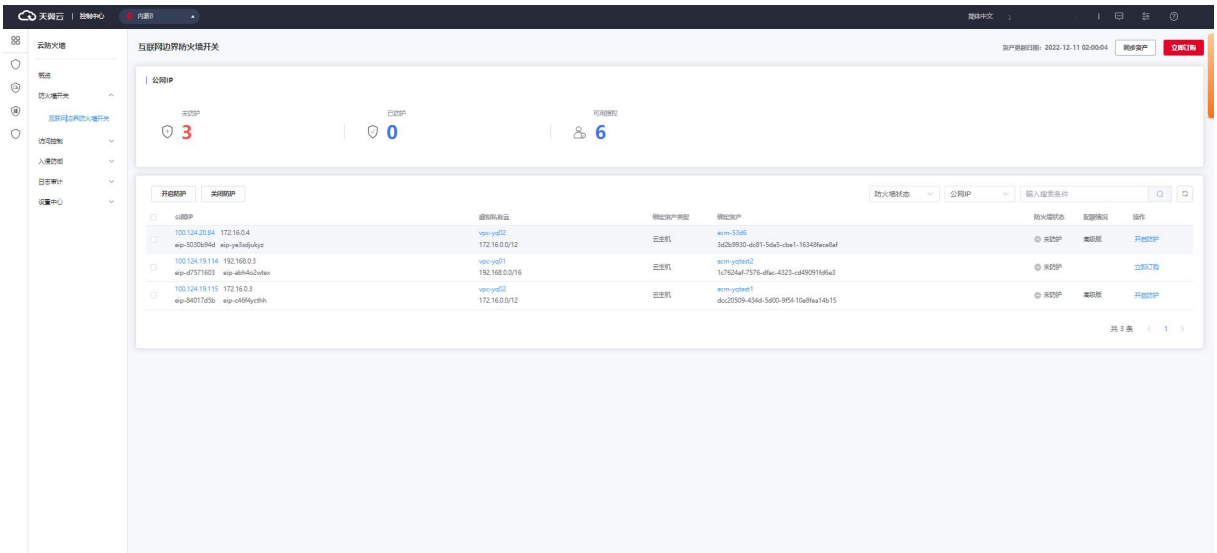
6. 最佳实践

6.1. C100 最佳实践

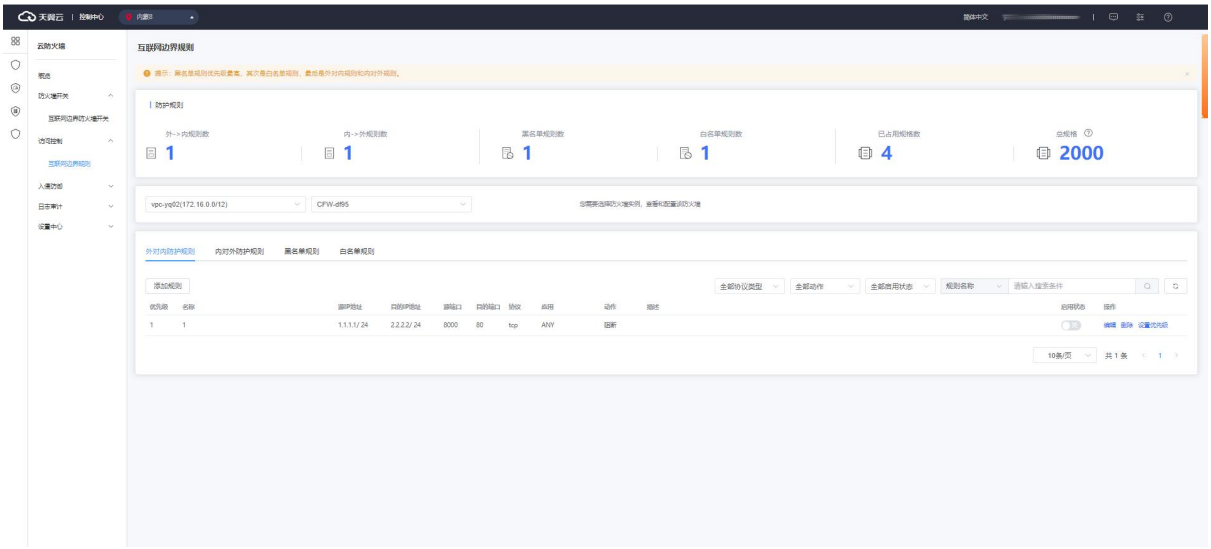
6.1.1. 云防火墙最佳实践

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：

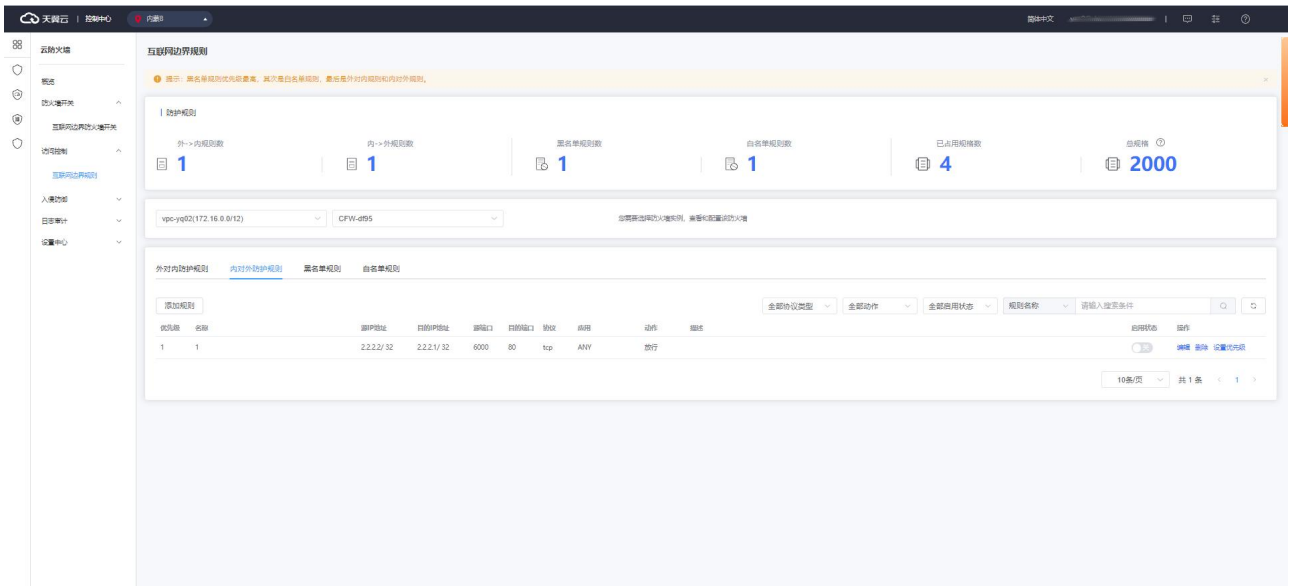


3. 配置外到内的访问策略：在“访问控制->互联网规则->外对内防护规则”页面可进行配置，如下图所示：



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。

6.1.2. 配置访问控制策略最佳实践

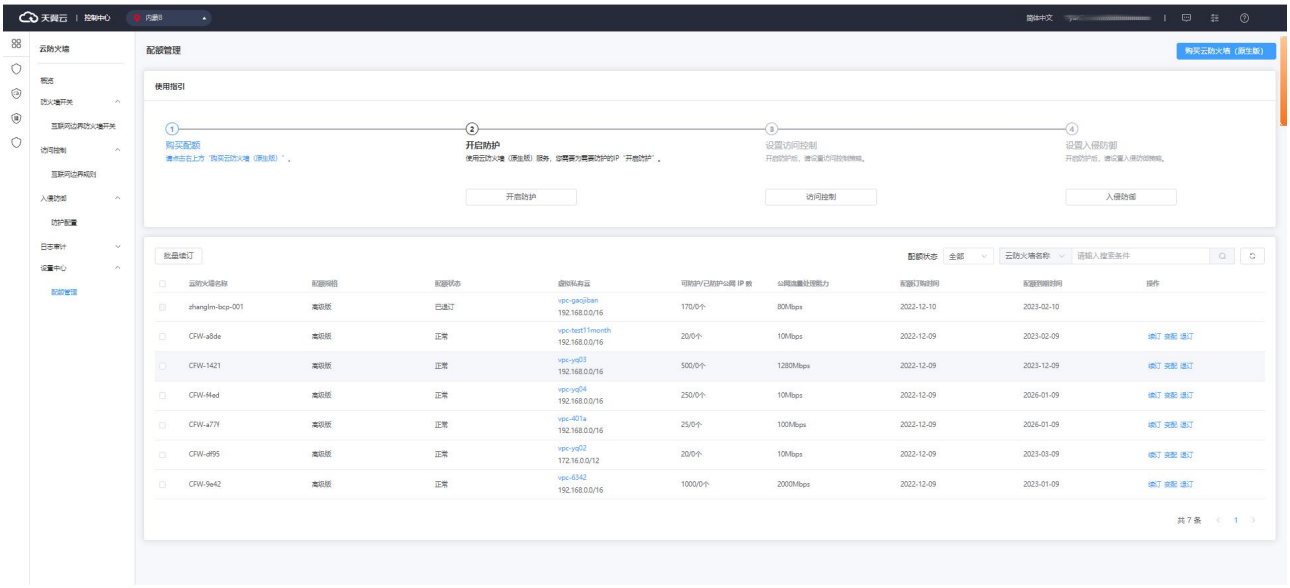
本节介绍互联网边界防火墙访问控制策略的推荐配置方法。

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）。

6.2. N100 最佳实践

6.2.1. IPv6 切换方案

前提条件

在使用云防火墙（原生版）- N100 型的 IPv6 方案之前，确保满足以下前提条件：

- 双栈云主机：承载云防火墙（原生版）- N100 型的云主机必须支持 IPv6 双栈，即同时支持 IPv4 和 IPv6 协议。如果当前云主机不支持双栈，请重新下单申请新的支持双栈的云主机。
- 子网启用 IPV6：在迁移过程（重新下单）中，承载云防火墙（原生版）- N100 型的云主机所在的子网必须启用 IPv6。确保子网设置正确，以避免开通问题。若未启用 IPv6，请在控制台中提前进行配置。

方案步骤

为确保顺利实施 IPv6 方案，建议遵循以下步骤：

1. 环境评估
   - 检查当前云主机的配置，确认其是否为 IPv6 双栈主机。
   - 评估现有应用和服务的 IPv6 兼容性，确保迁移不会影响业务。
2. 子网启用 IPv6

   在云平台控制台中，检查云防火墙（原生版）- N100 型主机需要使用的子网是否开启 IPV6，即确保子网已启用 IPv6。若尚未启用，请参考开启 IPv6 双栈进行设置。
3. 申请双栈主机

对于不支持 IPv6 的云防火墙（原生版）- N100 型主机，需重新下单云防火墙（原生版）- N100 型开通双栈云主机，确保其所选主机支持 IPv6，详细操作请参见购买 N100 实例。

4. 进行 IPv6 切换

   对于希望使用 IPv6 方案的现有用户，请按照以下步骤进行切换：

   a. 登录云防火墙（原生版）管理控制台。

   b. 点击实例列表操作列的“配置”，登录云防火墙（原生版）实例，进入配置界面。

   c. 根据需求完成云防火墙（原生版）IPV6 策略等配置。

   d. 业务割接。

5. 测试与验证

   完成配置后，进行全面的测试，以确保 IPv6 连接正常。验证云防火墙（原生版）- N100 型的安全策略是否有效应用于 IPv6 流量。

6. 监控与优化

   实施后，请定期监控 IPv6 流量，评估防火墙性能，并根据业务需求及时优化安全策略，以应对网络变化。

说明：

如需进一步支持，欢迎联系技术支持团队获取更多信息和帮助。

6.2.2. 双向访问控制

背景信息

云防火墙（原生版）作为云计算环境的边界网络安全，符合等级保护要求条例中边界安全访问控制要求项，能够实现内外网访问控制隔离等要求。

前期准备

用户需按业务需求整理好业务内外访问控制需求，整理点包含但不限于以下内容：

- 访问互联网业务的云主机信息，内网 IP 地址。

- 访问互联网业务是否存在限制，是否需要记录上网行为审计。
- 对外发布业务云主机信息，内网 IP 及对应公网 IP。
- 对外发布业务云主机的业务端口信息，使用协议，域名信息等。
- 对外业务或端口是否需要限制源地址访问，例如运维端口仅放行运维人员访问。

配置流程

云计算边界扩展针对云·边界安全有如下要求，要求边界安全能够实现访问控制、恶意代码防范、入侵防范等能力，以下配置流程可实现以上边界安全需求。

配置流程说明：

序号	子流程	配置内容
1	梳理业务映射关系	1. 访问互联网业务的云主机信息，内网 IP 地址，详情参考《云墙上线信息收集表》。 2. 访问互联网业务是否存在限制，是否需要记录上网行为审计。 3. 对外发布业务云主机信息，内网 IP 及对应公网 IP。 4. 对外发布业务云主机的业务端口信息，使用协议，域名信息等。 5. 对外业务或端口是否需要限制源地址访问，例如运维端口仅放行运维人员访问。 6. 是否有 WAF/CDN 业务访问，提供源站白名单。
2	配置网络接口	按照平台已添加的网卡进行网卡接口配置，登录云墙【网络】→【接口】→【接口配置】。
3	配置基础准备环境	按需配置对象薄、地址薄等信息，登录云墙【对象】→【服务薄】/【地址薄】。
4	配置出向 NAT 策略	确认需要访问互联网的云主机，进行 SNAT 配置【策略】→【NAT】→【源 NAT】。
5	配置入向 NAT 策略	确认需要访问互联网的云主机，进行 SNAT 配置【策略】→【NAT】→【目的 NAT】。
6	配置安全策略	确认需要进行过滤的访问对象，进行安全策略配置【策略】→【安全策略】→【新建】。

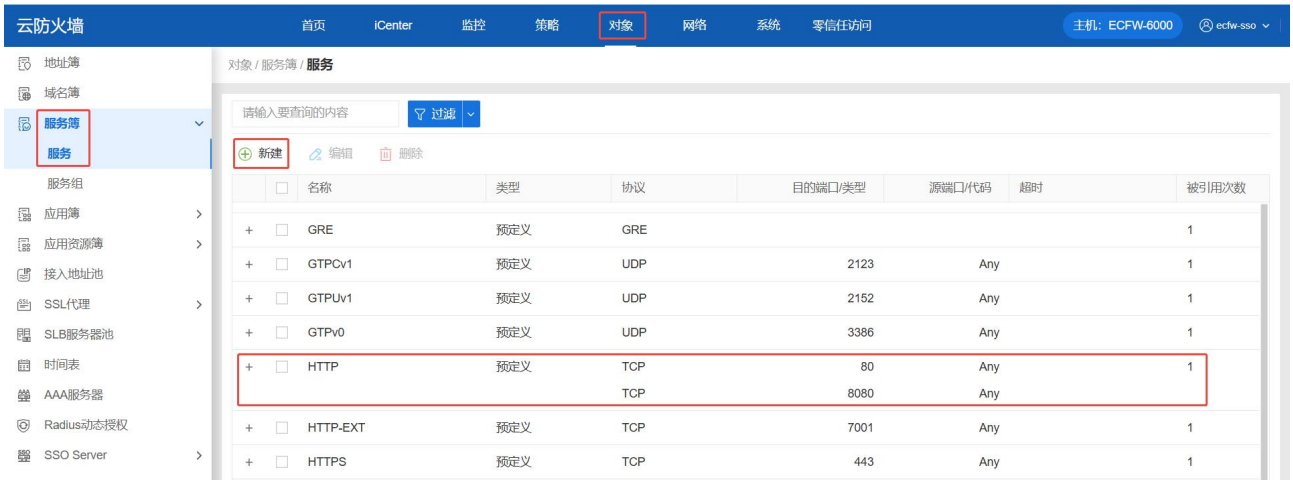
序号	子流程	配置内容
7	配置出向路由和平台路由	确认内网访问互联网的出接口地址，配置出向路由【网络】→【路由】→【源路由】。
8	配置业务割接	将弹性 IP 从云主机上解绑至云墙网卡即可。

配置内容

提前准备好对应内网服务器的端口服务薄及地址薄等相关对象信息。

服务薄相关配置

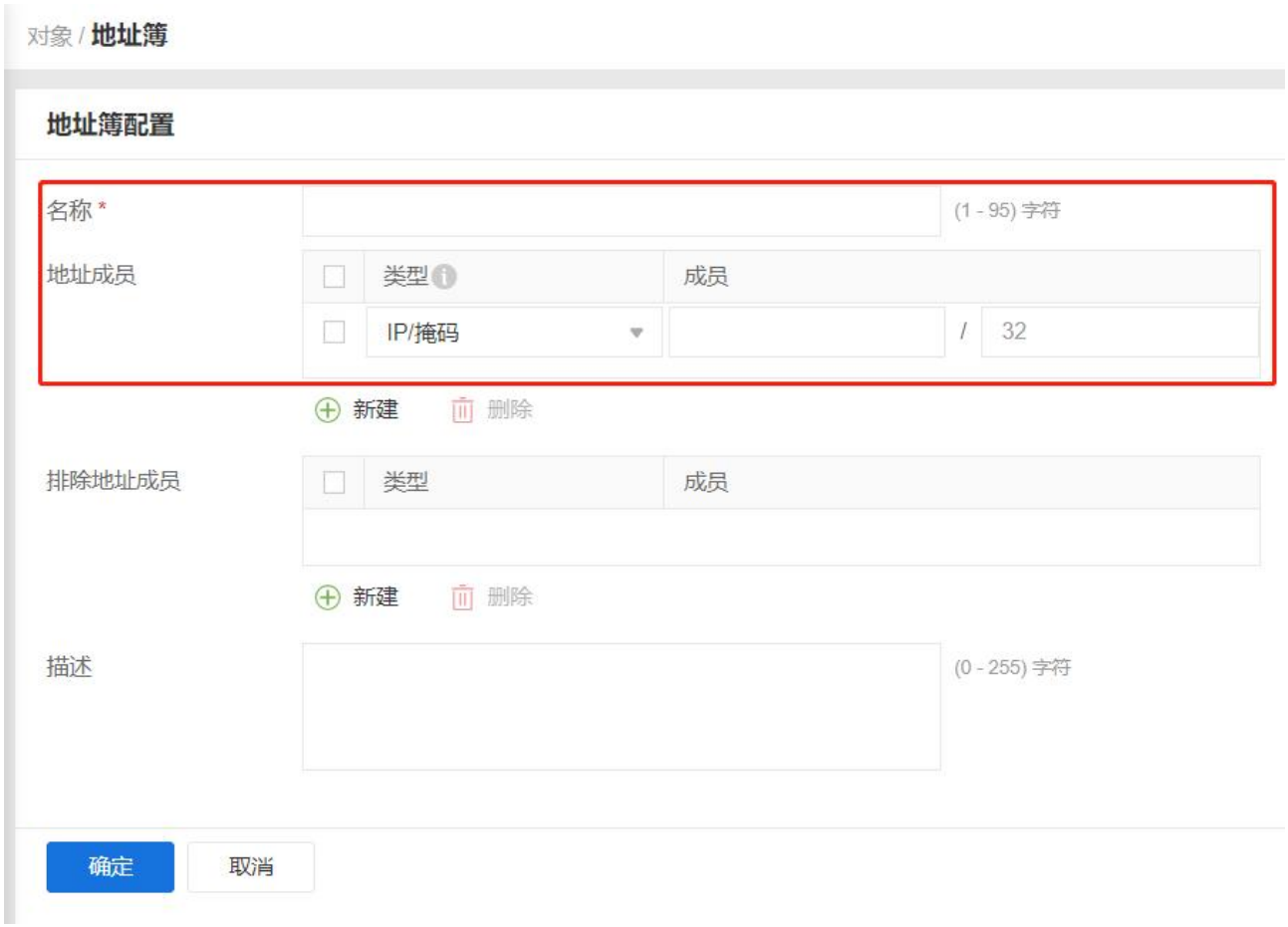
登录云墙控制台，进入【对象】→【服务薄】→【服务】，可直接引用内置或新建。



地址薄准备

登录云墙控制台，进入【对象】→【地址薄】。

单击“新建”，新建地址薄，输入名称和地址信息即可。



配置源/目的 NAT 策略配置

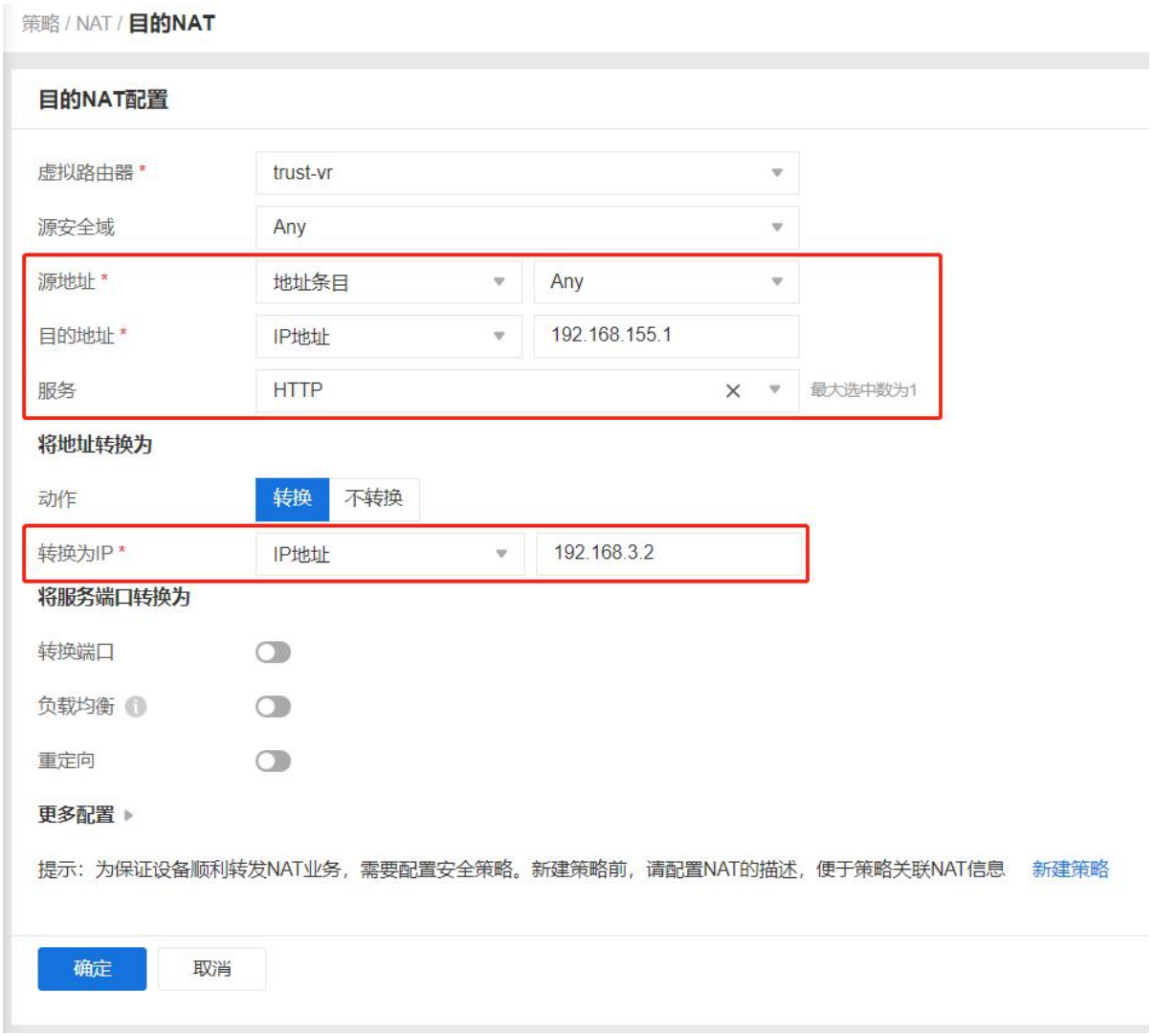
放行策略配置完成，需针对业务进行访问控制隔离配置，首先配置出站 SNAT 策略。

1. 打开菜单栏，【策略→NAT→源 NAT】，新建策略。

2. 打开菜单栏，【策略→NAT→目的 NAT】，单击“新建 > 高级配置”，新建策略。

参数	说明
源地址	依据真实业务确认是否限制源地址。

参数	说明
目的地址	防火墙网卡地址。
服务	业务需放行端口策略，调用服务簿。
转换为 IP	业务主机真实网卡地址。



配置安全策略

出入向地址转换策略配置完成后，需针对流量进行安全检测，该功能由安全策略实现。

打开菜单栏，“策略→安全策略→策略”，单击“新建 > 策略”，新建策略。

参数	说明
名称	自定义名称。
源安全域	安全域可根据业务情况选择。
源地址	源地址可根据业务情况选择。
目的地址	目的地址地址可根据业务情况选择，请输入防火墙网卡地址。
服务	根据业务主机开放端口选择服务。

策略配置

名称	1	(0 - 95) 字符
源安全域	Any	最大选中数为1
源地址	Any	最大选中数为1,024
目的安全域	Any	最大选中数为1
目的地址	Any	最大选中数为1,024
域名		域名簿最大选中数为8
用户		用户，用户组，角色最大选中数分别为8
服务	Any	最大选中数为1,024
应用		最大选中数为1,024
VLAN ID		最多配置32条

(多个VLAN ID 请用分号分割，例如1;2)

动作：允许 | 拒绝 | 安全连接

启用Web重定向

审计注释 (0 - 255) 字符

防护状态

病毒过滤	开	predef_middle
入侵防御	开	predef_default
URL过滤	关	
沙箱防护	开	predef_middle

数据安全

选项

配置出向路由和平台默认路由

登录云防火墙：【网络→路由→源路由】，单击“新建”。

参数	说明
源 IP	需要访问互联网的地址或网段。
下一跳	需要使用访问互联网的防火墙网卡接口。
网关	防火墙网卡的网关地址。

登录云平台控制台，虚拟私有云→VPC→路由表→新建，下一跳地址输入云防火墙（原生版）N100 型实例网卡地址即可。

6.2.3. SSL VPN 远程拨入

背景信息

用户存在远程拨入运维请求，但未购买天翼云平台 SSL VPN 服务，可使用云防火墙（原生版）N100 型实例的 SSL VPN 服务，该服务需单独配置。

前期准备

提供使用 SSL VPN 人员数量及人员账户信息。

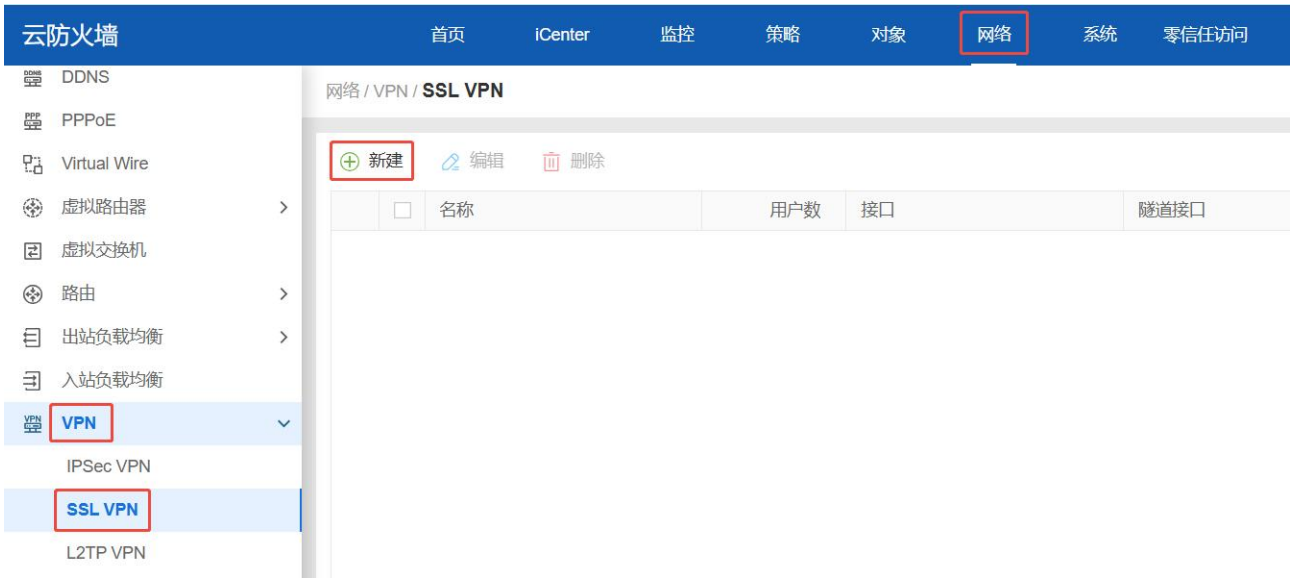
配置流程说明

序号	子流程	配置内容
1	梳理 VPN 用户及登录密码	梳理内部登录权限
2	创建 VPN 地址池	【网络】→【VPN】→【SSL VPN】→新建
3	创建用户	【对象】→【用户】→【本地用户】→新建

序号	子流程	配置内容
4	创建隧道接口	【网络】→【接口】→【新建】，编辑安全域及对应地址和链接隧道
5	配置安全策略	确认需要进行过滤的访问对象，进行安全策略配置 【策略】→【安全策略】→【新建】。

配置 VPN 地址池

打开【网络→VPN→SSL VPN】，单击“新建”，进入 SSL VPN 配置页面。



配置名称/接入用户：

配置“接入接口/隧道接口”：

新增地址池：新建-基本配置-起始 IP、终止 IP、掩码、DNS1。

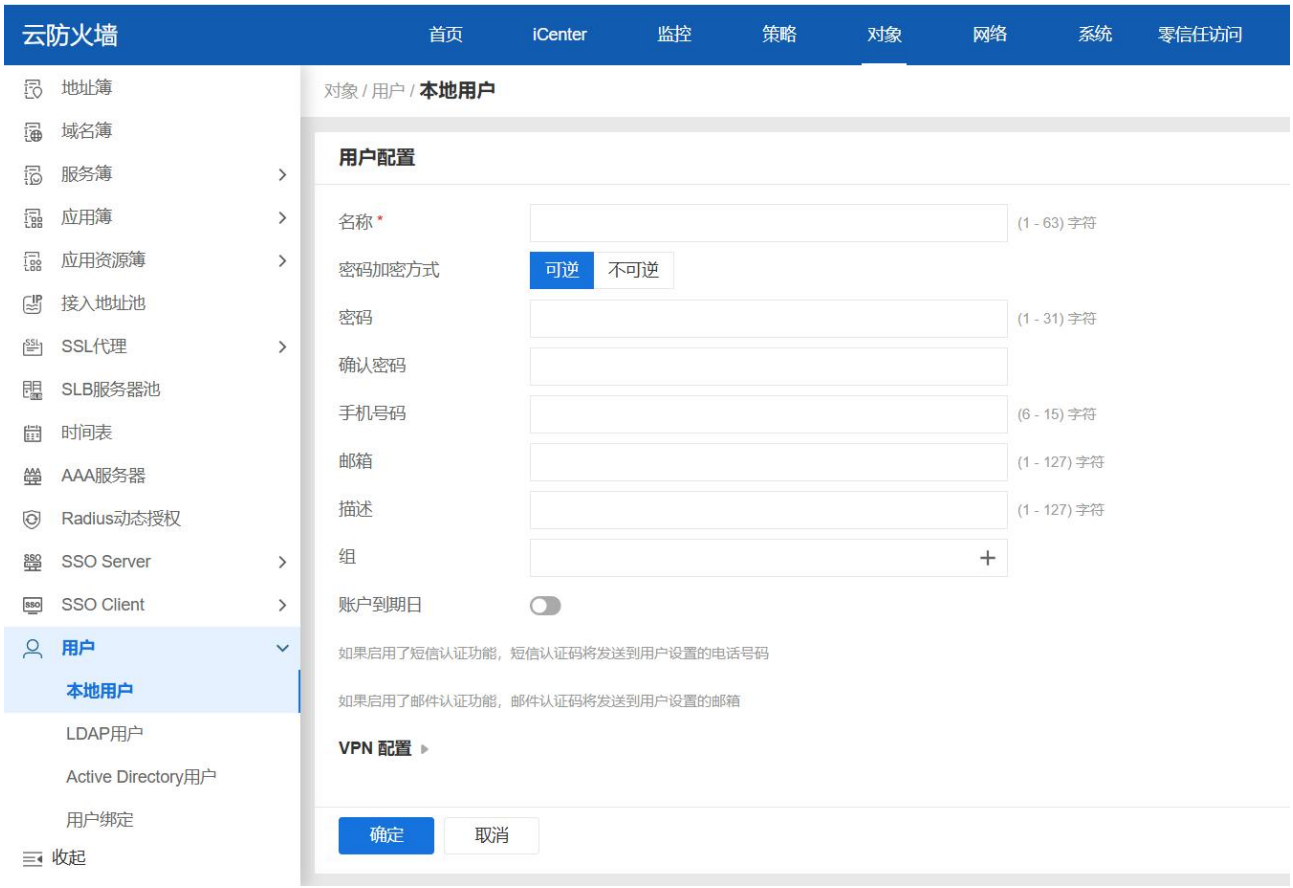
注意：

该地址池是用户拨入 VPN 后，用户可获取的 VPN 地址，必须与隧道接口中的地址在同网段，且不能覆盖。

隧道路由配置：

VPN 用户配置

登录云墙，打开【对象→用户→本地用户】，单击“新建 > 用户”，输入名称、密码、确认密码。

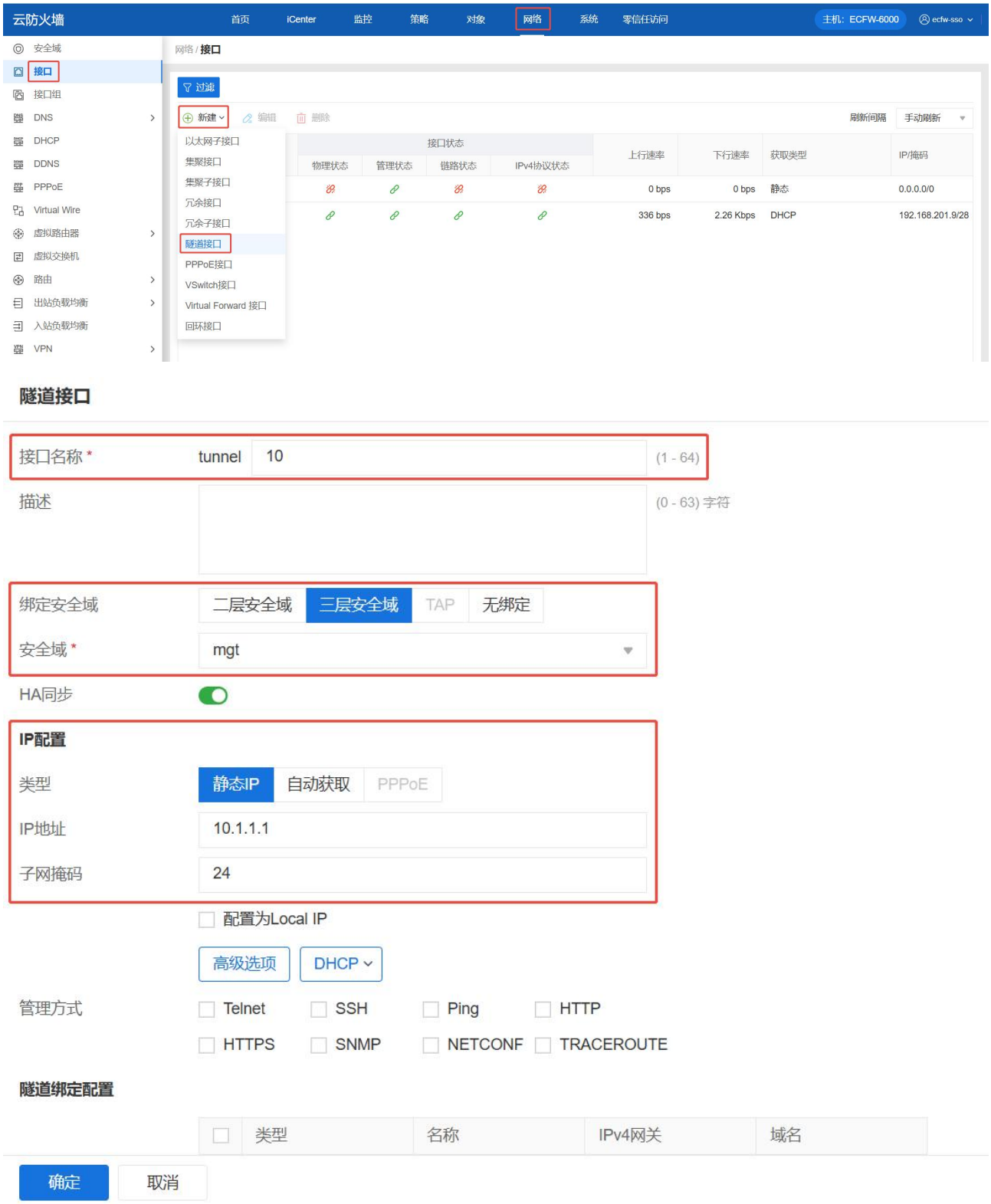


配置 VPN 安全域

打开【网络→安全域】，使用 VPN 安全域。

新建 SSL VPN 隧道接口

打开【网络→接口】，单击“新建 > 隧道接口”。



- 配置接口名称：tunnel10；
- 安全域：VPNHub；

- IP 地址配置：10.1.1.1/24。

注意：

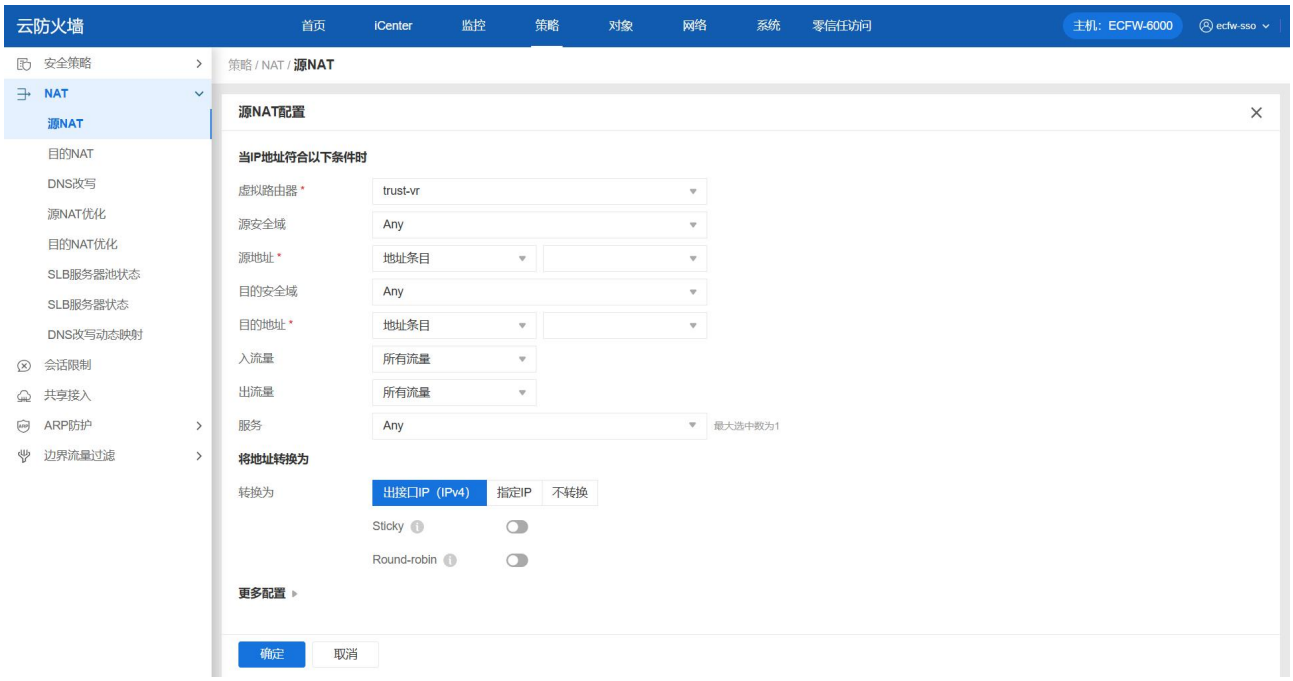
该 IP 地址是用于 VPN 登录时的网关地址，一般默认是 XX.XX.XX.1/24 的地址。

该地址网段涉及到下面 SSL VPN 地址池的配置，请根据自身网络进行规划。

逆向路由：关闭，防止出现环路。

配置出向策略

SNAT 配置：VPN 地址池转换为防火墙接口地址。



安全策略访问：VPN 安全域（被转换接口安全域）。

VPN 登录

1. 配置完成后，在 PC1 的浏览器中输入 https://IP:4433，并在弹出的登录页面输入用户名和密码，分别是“user_test”和“123”。点击“登录”后，页面弹出提示信息“此网站需要安装以下加载项：“Hillstone Networks，Inc.”中的“WebVPN.cab”...请单击这里”。

2. 鼠标右键单击此提示信息，并点击“为此计算机上的所有用户安装此加载项”。系统提示下载并安装 Hillstone Secure Connect，下载链接：https://www.hillstonenet.com.cn/support-and-training/hillstone-secure-connect/。
3. 安装完成后，安装 SSL VPN 拨号客户端，填写相应信息进行拨号后，即可访问内网业务，其中 SSL VPN 拨号客户端由云防火墙（原生版）工程师提供。

- 服务器地址：指本配置的 VPN 地址，具体内容由本单位管理员提供。
- 端口：指本配置的端口地址，具体内容由本单位管理员提供，默认为 4433。
- 用户名：指本配置的用户信息，具体内容由本单位管理员提供。
- 密码：指本配置的密码信息，具体内容由本单位管理员提供。

7. 常见问题

7.1. C100 常见问题

7.1.1. 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。

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。

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以及安全策略的防护。

- 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：云防火墙互联网边界防护的防护策略顺序为：黑名单规则 > 白名单规则 > 入向规则和出向规则 > 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：

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。

Q：云防火墙和安全组之间有什么区别？

- **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。

7.1.2. 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。

7.1.3. 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。

7.1.4. 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。

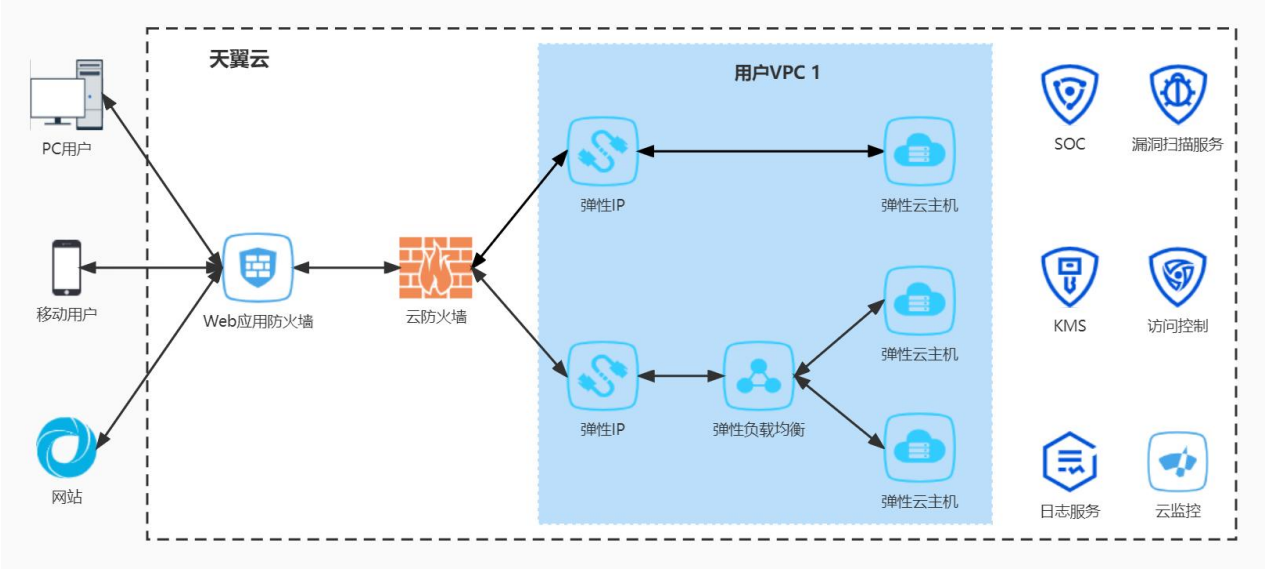
Q：入侵防御拦截模式开启后，是否会影响到云内网地址间的通信？

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。

7.1.5. 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。

7.2. N100 常见问题

7.2.1. 计费类

Q：N100 是否可以按月计费?

N100 支持按月/按年计费，最低订购时长为 1 个月。

Q：云主机和 N100 计费是否重复?

云主机订购费用和 N100 的计费是不同步的，云主机计算属于资源计算，需要按照平台云主机计费标准；N100 属于服务计费，会根据使用规格、时长、功能等项目进行计费。

Q：我已经购买了云 N100，是否意味着已开启安全防护?

不是。购买成功后还需要一系列的配置才能开启安全防护，例如准备承载机资源、导入授权、配置引流、开启安全防护策略、设置告警通知等配置。

7.2.2. 购买类

Q：哪些资源池可以支持开通 N100?

N100 支持的资源池请以管理控制台为准。

开通流程：在选择资源池节点后，您可以登录天翼云官网，按照 N100 的开通流程进行操作。

影响面：开通 N100 可能会对您的网络拓扑结构产生一定的影响。在执行开通操作之前，建议您仔细规划，并在可能的情况下在非业务高峰期进行操作，以减少对正常业务的影响。

注意：

在开通 N100 时，请仔细阅读相关的注意事项和配置要求。确保您的网络环境和业务需求符合产品的要求，以便最大程度地发挥防火墙的作用。

Q：如何选择需要购买的产品规格和功能?

需要用户自行评估业务情况，可通过以下内容进行参考：

- 规格选择：计算通过 N100 安全产品的弹性 IP 总带宽值，不高于 N100 安全产品各规格限制值。
- 功能选择：有安全防护需求需开通扩展功能，如病毒过滤、URL 过滤及 C&C 防护。

Q：N100 到期后是否可自行续订?

是的，您可以自行发起 N100 的续订申请，确保您的业务在产品到期后不受到中断。以下是相关的详细信息和操作指南：

- 续订申请发起：为了确保您的 N100 服务不中断，建议您在产品到期前至少提前 3 个工作日主动发起续订申请。续订申请可以通过我们的在线平台或与客户经理联系来完成。
- 申请时间：提前提交续订申请是至关重要的，这样我们的团队有足够的时间来处理您的请求，确保续订在产品到期之前得以完成。这有助于避免因产品过期而导致的业务中断。
- 在线平台操作：如果您选择通过在线平台进行续订申请，请登录您的云账户，点击 N100 产品的续订选项，并按照系统提示完成续订流程。确保在续订过程中提供准确的信息，以避免不必要的延误。
- 注意事项：在续订申请过程中，请仔细阅读相关条款和条件，确保您了解续订期间可能涉及的费用、服务升级选项等细节。如果有任何疑问，可以咨询客户经理或技术支持团队。
- 业务影响：请注意，如果未在到期前完成续订申请，可能会导致 N100 服务中断，影响业务转发。为了避免不必要的风险，请务必按时发起续订申请并遵循相应的操作流程。

Q：同一天翼云账号已商用，后期是否拥有试用权限?

没有试用权限。商用订单一旦开始，该天翼云账号不再享有试用权限。

- 解决方案选择：如果您需要继续测试产品或服务，但不希望立即进行商用订单，您可以考虑与我们的销售团队或客户经理合作，探讨其他解决方案。
- 业务影响：试用权限的取消可能对您的业务测试和决策过程产生一定的影响。因此，在进行商用订单之前，请确保您已经完成了充分的评估和试用，以避免可能的问题。

注意：

在进行商用订单之前，请确保您已充分评估和测试所需的产品，以避免购买后后悔或发现与业务需求不匹配的情况。商用订单一旦生效，将被视为最终的购买决策。

Q：受理单一直处于开通状态，可以正常使用 N100?

开通状态仅表示订单目前的处理状态，并不影响客户正常使用 N100 安全产品。

- 开通状态：开通状态是指您的受理单正在处理中，可能涉及到 N100 的部署、授权导入以及其他相关的操作。这是一个中间状态，与您正常使用产品的权限没有直接关系。
- 使用 N100： 客户在受理单处于开通状态时，仍然可以正常使用 N100。在完成相应的部署、授权导入以及业务割接等操作后，产品将会被正确配置并生效。
- 业务割接： 如果您的订单涉及到业务割接，可能需要特别注意相关操作，以确保在切换过程中不影响到您的正常业务运行。我们建议在割接前仔细计划，并可能在非业务高峰期执行。

注意：

在使用过程中，如果您遇到任何技术或操作方面的问题，请随时联系我们的技术支持团队。我们将全力支持您解决任何可能影响您正常使用的问题。

Q：云墙 VPN 功能是否可以免费使用?

云墙 VPN 功能支持免费使用。这是云墙的基础功能模块之一，为用户提供安全、可靠的虚拟专用网络连接。以下是相关功能详细信息：

- 基础功能模块：云墙 VPN 功能是 N100 的基础功能之一，旨在为用户提供安全的远程访问和站点到站点的连接服务。
- IPSEC VPN 链路：根据不同的版本，IPSEC VPN 支持的链路条数可能有所不同。用户可以根据业务需求选择适当的版本。
- SSL VPN 账号限制：默认情况下，SSL VPN 支持最多 5 个账号同时在线。如果您的业务需要更多同时在线账号，您可以联系天翼云客服进行进一步的咨询和配置。
- 扩展服务：如果您的业务需求超出了免费版本所提供的功能，我们提供了更高级的版本和扩展服务，以满足不同用户的需求。您可以与天翼云客服联系，了解更多关于高级版本和扩展服务的信息。

7.2.3. 操作类

Q：N100 如何开启防护功能?

- 登录管理界面：首先，使用管理员凭据登录到 N100 的管理界面，可以在 Web 浏览器中输入设备的管理方式来访问 N100 管理界面。
- 导航到防护功能：在管理界面对象中，找到防护功能（IPS、AV、URL、OQS、IP 信誉库、僵尸网络防御、云沙箱）进行防护功能模版的配置。
- 启用防护策略：选择外网卡的安全域（网络-安全域）或安全策略，然后开启且调用所需的安全功能模板。

- 监控和日志记录：启用监控和日志记录功能（监控-日志-编辑对应日志-开启日志缓存），以跟踪安全事件、威胁检测以及系统性能。这有助于实时监视和分析潜在的威胁。
- 测试和优化：在启用防护功能后，建议进行测试以确保其正常运行，并进行必要的优化，以适应业务需求。

Q：N100 无法启动或连接怎么办?

首先确认 N100 所防护的业务是否正常，如果正常可以先排查一下 N100 管理 EIP 是否被解绑（解绑了会无法通过公网进行管理），是否调整了安全组限制了管理端口（安全组限制会导致公网机内网进行管理）。如果业务不正常，急需恢复业务，请将云主机的 EIP 从 N100 上解绑，绑至对应业务云主机上，让 VPC 南北向流量绕过 N100，进行业务的恢复（如果此时业务云主机修改了网关为 N100 的地址，那么请修改 VPC 内所有业务云主机的网关为默认网关，网关还请参照虚拟私有云（VPC）内的子网信息）。

其次，天翼云控制台云主机列表找到 N100 主机，进行远程登录，看是否能打开正常运行，查看配置是否正常。

最后，如果依旧存在问题，请联系客服。

Q：N100 如何更新特征库?

登录 N100 的 UI 管理界面，找到系统-升级管理-特征库升级-点击对应需要升级的特征库-开启自动升级配置-配置好后点击确认并在线升级（建议时间设置在凌晨）。

下列条件会导致 N100 无法更新特征库，在检查完毕之后点击立即在线升级：

- N100 无法访问互联网。
- N100 上缺少 DNS 的相关配置。
- N100 上缺少对应功能的许可。

Q：N100 如何导入授权?

N100 订购成功后，会有技术工程师联系进行授权导入，也可以自行授权导入自行导入。

导入方式如下：

登录 N100 CLI 界面，输入以下命令导入授权，exec license install 证书内容字符串（证书会通过天翼云工单系统交互或线下联系发送），授权模块需单独进行导入，导入完成后，进行重启即可，以上操作有任何问题，均可向天翼云客服提交工单咨询。

Q：N100 如何查看威胁日志?

威胁日志的作用是记录和跟踪计算机网络和系统中的潜在威胁、攻击和异常活动，以便及时检测、调查、分析和应对安全事件。威胁日志的查看可登录 N100WEB UI 页面，找到 UI 界面监控-日志-威胁日志进行详细信息的查看。首页也会显示当前安全威胁日志和高危主机 IP 地址等，可依据需求进行过滤查询。

Q：N100 是否支持六个月日志留存?

六个月的日志保留期限通常是为了合规性、安全审计和犯罪调查需要而设定的。而 N100 日志主要留存在内存中，可存容量有限，不支持六个月留存，需要日志审计或者日志服务器配置 snmp 或者 syslog 进行日志保存， 具体配置为登录 N100 的 UI 界面→监控→日志→日志配置→日志服务器配置→新建→填写日志服务器信息对日志进行发送。

Q：N100 可以防护多个 VPC 之间的流量吗?

防火墙可以实现多个 VPC 流量防护。

前提条件如下：

VPC 的虚拟路由器需要支持写全 0 默认路由，配置下一跳为对等连接，且写了默认路由不影响直接绑定 EIP 的业务主机转发。

该方式会打通原本隔离的 2 个 VPC 网络，能接受 2 个 VPC 网络打通带来的安全风险。

Q：N100 是否支持上网行为审计?

支持，例如 QQ 用户、微信用户、微博用户的使用情况。N100 在上网行为审计方面的功能相对有限，可能不如专门的审计工具或高级审计解决方案强大。如果您有特定的审计需求，可能需要考虑额外的审计

工具以满足您的要求。然而，N100 通常专注于网络安全和流量管理，提供基本的审计功能以辅助安全监控和合规性要求。

Q：N100 默认账号密码?

强烈建议在 N100 安装交付后立即更改默认账号和密码以提高安全性。默认账号和密码是保密信息，为了确保您的网络的安全，无法在此提供默认凭据。

请在天翼云官网上提交 N100 的技术支持工单联系支持团队以获取有关如何更改及默认凭据的详细信息。保护默认凭据的机密性对于网络安全至关重要。

Q：是否支持流量统计分析?

支持流量统计分析功能。它可以提供外部访问和主机外联流量的统计数据，帮助您了解网络流量的模式、趋势、来源和目标。然而请注意，N100 的主要焦点是在流量统计方面，而不是深入的流量分析。对于更深入的分析需求，您可能需要考虑使用专门的流量分析工具或安全解决方案。

7.2.4. 管理类

Q：N100 过期后无法配置?

N100 授权过期后会锁定配置，需导入续订授权后重启恢复。如过期时间较长会影响业务正常访问。

建议：过期后还请尽快续订，如不续订，还请解绑弹性 IP 至业务主机，防止出现业务影响。

Q：N100 如何创建管理员用户?

要创建管理员用户，请登录 N100 的 Web 管理页面，导航到系统-设备管理选项，然后选择管理员管理。在此处，您可以新建管理员用户，分配唯一用户名和强密码，以及为其分配适当的角色和权限。

注意：

创建管理员用户涉及系统权限，因此确保定期审计管理员用户，启用多因素身份验证，并使用最小权限原则来降低管理上的风险。

Q：N100 是否满足三权分离?

三权分离用于确保权力不会集中在一个单一的实体或个人手中，以防止滥用权力、促进监督和平衡，从而维护公共机构的透明性和效力。在信息安全领域，三权分离原则通常应用于管理系统和数据的访问和操作，以保护网络安全和防止内部滥用权力。

N100 提供内置的管理员、操作员和审计员权限，允许实现三权分离。您可以登录 N100 的 Web 管理页面，导航到系统-设备管理选项，然后选择管理员管理并分配相应权限，以确保合适的角色和职责，但需要定期审计和管理用户权限，以最大程度地减少潜在的管理上风险。