云防火墙

用户使用指南

天翼云科技有限公司

目 录

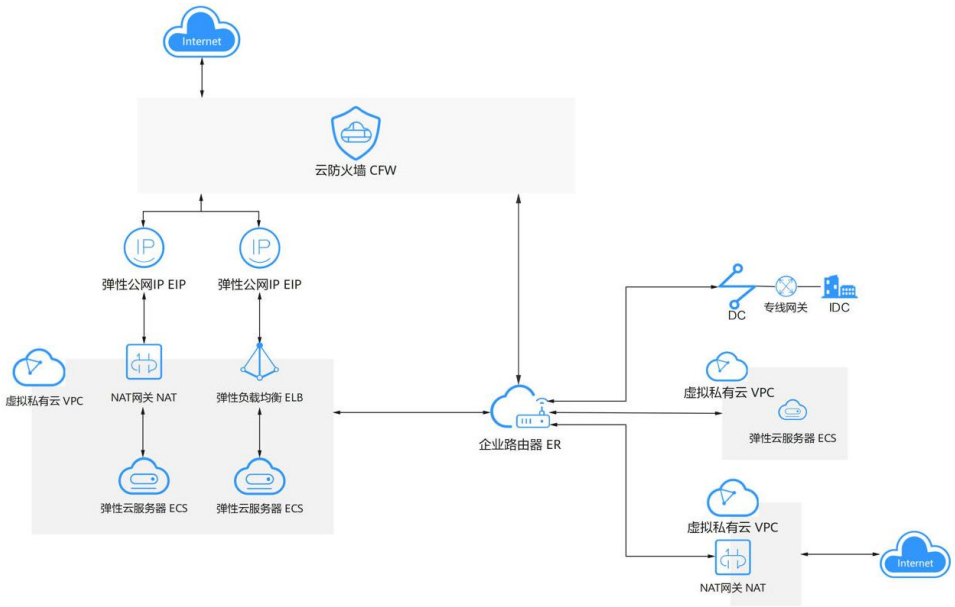
1 产品简介

1.1 产品定义及优势

云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC 边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持 AI 提升智能防御能力满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。

- 互联网边界：互联网边界是云资产与互联网之间的界限，管控入云（互联网访问云资产）和出云（云资产主动访问互联网）的通信流量。
- VPC 边界：VPC 边界是 VPC 与线下数据中心 IDC、VPC 与 VPC 之间的界限，管控内部业务互访。

定位全景图



智能防御

CFW 通过安全能力积累和全网威胁情报，提供 AI 入侵防御引擎对恶意流量实时检测和拦截，与安全服务全局联动，防御木马蠕虫、注入攻击、漏洞扫描、网络钓鱼等攻击。

灵活扩展

CFW 可对全流量进行精细化管控，包括互联网边界防护、跨 VPC 的流量，防止外部入侵、内部渗透攻击和从内到外的非法访问；集群部署高可靠，满足大规模流量的安全防护。

极简应用

云防火墙作为云原生防火墙，支持一键开启，多引擎安全策略一键导入，资产自动秒级盘点，操作页面可视化呈现，大幅提高管理和防护效率。

支持的防护对象

防护类型	防护对象	相关文档
互联网边界	弹性公网 IP（EIP），支持防护 EIP 和绑定了 EIP 的资源，例如弹性云服务器（ECS）、NAT 网关（NAT）、弹性负载均衡（ELB）等。	3.3.1 开启互联网边界流量防护
VPC 边界	企业路由器（ER）支持绑定的云资源，例如虚拟私有云（VPC）、虚拟网关（VGW）、虚拟专用网络（VPN）等。	3.3.2 开启 VPC 边界流量防护

支持的访问控制策略

- 基于五元组的访问控制。即源 IP 地址、目的 IP 地址、协议号、源端口、目的端口。
- 基于域名的访问控制。
- 基于 IPS（intrusion prevention system，入侵防御系统）设置访问控制。IPS 支持观察模式和拦截模式，当您选择拦截模式时，云防火墙根据 IPS 规则检测出符合攻击特征的流量进行拦截。
- 支持对 IP 地址组、黑名单、白名单设置 ACL 访问控制策略。

相关文档

如果需要了解云防火墙的计费内容，请参见 2 计费说明。

如果需要了解详细功能和各版本差异请参见 1.3 产品功能。

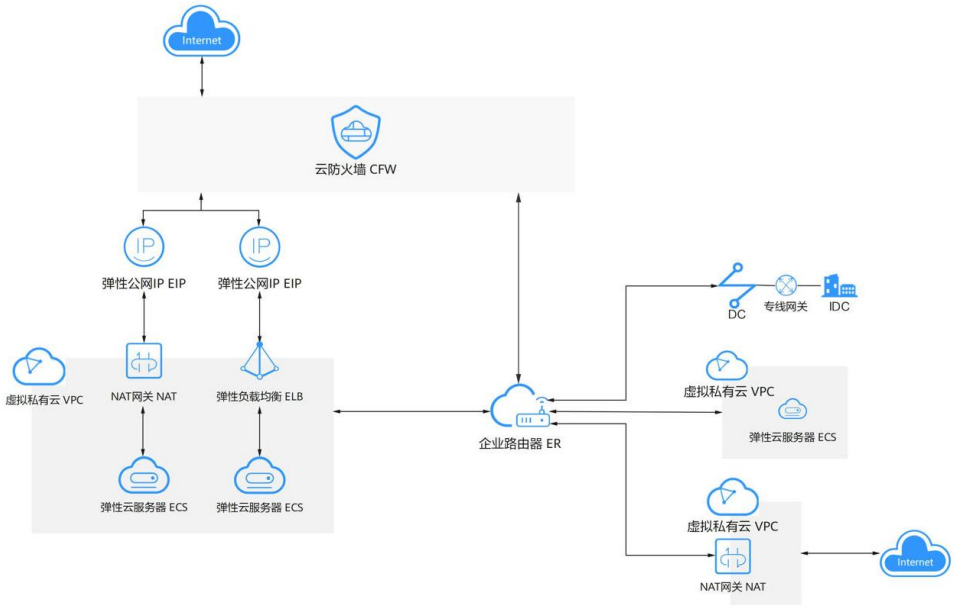
如果需要了解云防火墙的使用流程，请参见《云防火墙快速入门》中“入门指引”章节。

1.2 应用场景

云上资源统一安全管控

提供资源的多场景防护，动态感知流量变化趋势，全面保障云上资产安全。

- 互联网边界：互联网边界是云资产与互联网之间的界限，管控入云（互联网访问云资产）和出云（云资产主动访问互联网）的通信流量。
- VPC 边界：VPC 边界是 VPC 与线下数据中心 IDC、VPC 与 VPC 之间的界限，管控内部业务互访。



外部入侵防御

新型攻击手段层出不穷，网络安全事件频发，云防火墙提供对已开放公网访问的服务资产进行安全盘点，支持一键开启入侵检测与防御，智能拦截恶意入侵、病毒攻击等行为。

主动外联管控

内网主机非法外联导致敏感数据泄露，云防火墙提供基于域名等多维度的访问控制，通过精细化策略阻断非法外联事件，有效阻断恶意连接行为，保护资产安全。

VPC 间互访控制（专业版支持）

内网非法越界访问导致横向渗透攻击范围扩大，云防火墙支持 VPC 间流量的访问控制，实现内部业务互访活动的可视化与安全防护。

等保合规

云防火墙可满足《网络安全等级保护 2.0》标准中的多项要求，包括区域边界防护、网络入侵防范、网络访问控制、安全日志审计等检查项目。

1.3 产品功能

为满足不同场景下的防护需求，云防火墙提供了“标准版”、“专业版”供您使用，包括访问控制、攻击防御、流量分析以及日志审计等功能。

说明

本文表格中使用的标识说明：

- √：表示在当前版本中支持。
- ×：表示在当前版本中不支持。

总览

总览呈现云上资产的整体防护和安全策略配置情况，助您全面了解资产的安全状态。

表 1-1 总览功能介绍

功能名称	功能描述	标准版	专业版（包周期）
总览	实时展示云上资产的安全防护状态，帮助您全面了解攻击事件和异常流量等安全风险。	√	√

资产管理

云防火墙提供对云上资产的安全防护，有效降低安全风险。

表 1-2 资产管理功能介绍

资源名称	功能描述	标准版	专业版（包周期）
IPv4	支持对 IPv4 资产的防护	√	√
IPv6	支持对 IPv6 资产的防护	√	√
EIP	云防火墙通过对弹性公网 IP（EIP）的防护实现互联网边界流量的防护。	√	√
VPC（私网IP）	云防火墙通过对虚拟私有云（VPC）的防护实现 VPC 和 VPC 之间、本地数据中心（IDC）和云上 VPC 之间流量的防护。	×	√

表 1-3 云上资产的防护规格

功能名称	标准版	专业版（包周期）

功能名称	标准版	专业版（包周期）
防护的公网 IP（EIP）数量	20 个（可扩容，最大扩容至 2000 个）	50 个（可扩容，最大扩容至 2000 个）
防护的 VPC 数量	×	2 个（可扩容，最大扩容至 100 个）
互联网边界防护带宽	10Mbps（可扩容，最大扩容至 5,000Mbps）	50Mbps（可扩容，最大扩容至 5,000Mbps）
VPC 边界防护带宽	×	200Mbps（随 VPC 数量扩容）

访问控制

访问控制策略通过指定的 IP 地址、端口等参数有效地帮助您精细化管控云上资源的流量。

表 1-4 访问控制功能介绍

功能名称	功能描述	标准版	专业版（包周期）
防护规则	基于 IP 地址、域名、域名组、地理位置等方式灵活管控访问流量。	√	√
黑/白名单	基于五元组精确管控特定流量。	√	√
策略助手	快速查看防护规则的命中情况，及时调整防护规则。	√	√

攻击防御

攻击防御提供网络攻击防护、敏感目录扫描、拦截病毒文件等功能。

表 1-5 攻击防御功能介绍

功能名称	功能描述	标准版	专业版（包周期）

功能名称	功能描述	标准版	专业版（包周期）
入侵防御（IPS）	结合多年攻防积累的经验规则，针对访问流量进行检测与防护，有效保护您的资产。 根据内置的 IPS 规则库，提供威胁检测和漏洞扫描。支持检测流量中是否含有网络钓鱼、特洛伊木马、蠕虫、黑客工具、间谍软件、密码攻击、漏洞攻击、SQL 注入攻击、XSS 跨站脚本攻击、Web 攻击；以及检测是否存在协议异常、缓冲区溢出、访问控制、可疑 DNS 活动及其它可疑行为。 • 基础防御规则库支持手动修改防护动作。 • 基础防御规则库支持通过“规则 ID”、“特征名称”、“风险等级”、“更新年份”、“CVE 编号”、“攻击类型”、“规则组”、“当前动作”查询规则信息。	√	√
虚拟补丁	在网络层级为 IPS 提供热补丁，实时拦截高危漏洞的远程攻击行为，同时避免修复漏洞时造成业务中断。	√	√
自定义 IPS 特征库	当内置的 IPS 规则库无法满足需求时，CFW 支持自定义 IPS 特征规则，添加后，CFW 将基于签名特征检测数据流量是否存在威胁。 自定义 IPS 特征支持添加 HTTP、TCP、UDP、POP3、SMTP、FTP 的协议类型。	×	√
敏感目录、反弹 Shell	• 敏感目录扫描防御：防御对用户主机敏感目录的扫描攻击。 • 反弹 Shell 检测防御：防御网络上通过反弹 shell 方式进行的网络攻击。	√	√
病毒防御（AV）	通过病毒特征检测来识别和处理病毒文件，避免由病毒文件引起的数据破坏、权限更改和系统崩溃等情况发生，有效保护您的业务安全。 病毒防御功能支持检测 HTTP、SMTP、POP3、FTP、IMAP4、SMB 的协议类型。	×	√
安全看板	快速查看攻击防御功能的防护信息，及时调整 IPS 防护。	√	√

流量分析

流量分析展示当前防火墙实例防护的流量数据。

表 1-6 流量分析功能介绍

功能名称	功能描述	标准版	专业版（包周期）
流量分析	基于会话展示云上资产的 TOP 流量数据。	√	√

日志审计

日志审计支持记录攻击事件的详细信息、访问控制策略的命中详情以及经过防火墙的所有流量。

表 1-7 日志审计功能介绍

功能名称	功能描述	标准版	专业版（包周期）
日志查询	防火墙提供 7 天的日志记录，助您事件追溯和深入分析。	√	√
日志管理	将日志转储到云日志服务（Log Tank Service，简称 LTS）中，支持查看 1~365 天的日志记录。	√	√

系统管理

系统管理提供告警通知、DNS 配置、安全报告等功能，帮助您管理和维护云上资产的安全，及时发现异常情况。

表 1-8 系统管理功能介绍

功能名称	功能描述	标准版	专业版（包周期）
告警通知	您可以通过云防火墙服务对攻击信息、流量超额预警等事件进行通知设置。开启告警通知后，CFW 可将触发的信息通过您设置的接收通知方式（例如邮件或短信）发送给您。	√	√
DNS 配置	通过域名服务器解析并下发 IP 地址。	√	√
安全报告	生成日志报告，及时掌握资产的安全状况数据。	√	√

1.4 使用限制

本文介绍云防火墙 CFW 服务在使用过程中的约束和限制。

CFW 使用限制

- 仅支持对部署在云平台内的业务提供防护，不支持跨云使用。
- 支持弹性公网 IP EIP 的流量防护，不支持全域弹性公网 IP G-EIP、API 网关 APIG 绑定的 EIP 的流量防护。
- VPC 边界流量防护功能依赖企业路由器 ER 服务引流，使用该功能时，需确保账号下至少有一个企业路由器。
- 云防火墙不支持防护中文域名。

防护策略配额限制

- 一个防火墙实例最多添加 20,000 条防护策略（防护规则和黑白名单），同时黑白名单限制如下：
  - 一个防火墙实例最多添加 2,000 条黑名单。
  - 一个防火墙实例最多添加 2,000 条白名单。
- 防护规则中的引用限制如下：
  - 最多添加 20 个“IP 地址”（源和目的各 20 个）。
  - 最多关联 2 个“IP 地址组”（源和目的各 2 个）。
  - 最多关联 5 个服务组。
- 成员组
  - IP 地址组
    - 每个防火墙实例下最多添加 3,800 个 IP 地址组。
    - 每个 IP 地址组中最多添加 640 个 IP 地址成员，且单次最多可添加 100 个 IP 地址成员。
    - 每个防火墙实例下最多添加 30,000 个 IP 地址。
  - 服务组
    - 每个防火墙实例下最多添加 900 个服务成员。
    - 每个防火墙实例下最多添加 512 个服务组。
    - 每个服务组中最多添加 64 个服务成员。
  - 域名组
    - 域名组中所有域名被“防护规则”引用最多 40,000 次，泛域名（例如：*.example.com）被“防护规则”引用最多 2000 次。
    - **应用域名组（七层协议解析）**
      - 每个防火墙实例下最多添加 500 个域名组。
      - 每个防火墙实例下最多添加 2500 个域名成员。
      - 每个应用域名组中最多添加 1500 个域名成员，且单次最多可添加 500 个域名成员。
    - **网络域名组（四层协议解析）**

□ 每个防火墙实例下最多添加 1000 个域名成员。
□ 每个网络域名组中最多添加 15 个域名成员。
□ 每个域名组最多支持解析 1500 条 IP 地址。
□ 每个域名最多支持解析 1000 条 IP 地址。

基础防御 IPS 限制

- 修改基础防御规则动作
  - 最多可修改 3000 条规则为“观察”。
  - 最多可修改 3000 条规则为“拦截”。
  - 最多可修改 128 条规则为“禁用”。
- 自定义 IPS 特征
  - 仅专业版支持自定义 IPS 特征。
  - 最多支持添加 500 条特征。

日志数据限制

- 云防火墙支持查看 7 天以内的日志数据，如果需要记录并查看 1-365 天的日志数据，您可以将单类或者多类日志记录至云日志服务 LTS 中。
- 单个日志单次最多支持导出 100,000 条记录。

1.5 与其它服务的关系

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。需要拥有 Tenant Administrator 权限的用户才能拥有 CFW 服务的操作权限（包括云资源授权，资产管理以及执行资产检测任务等）。如需开通该权限，请联系拥有 Security Administrator 权限的用户。

与弹性公网 IP 的关系

弹性公网 IP（Elastic IP，简称 EIP）提供独立的公网 IP 资源，包括公网 IP 地址与公网出口带宽服务。

云防火墙通过对弹性公网 IP 的防护实现互联网边界流量的防护。

与虚拟私有云的关系

虚拟私有云（Virtual Private Cloud，VPC）是您在云上的私有网络，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。

云防火墙支持防护 VPC 边界的流量，例如 VPC 与 VPC 之间、云上 VPC 与云下 IDC 之间。

与 NAT 网关的关系

NAT 网关（NAT Gateway）提供公网 NAT 网关和私网 NAT 网关。公网 NAT 网关为 VPC 内的云主机提供 SNAT 和 DNAT 功能，可轻松构建 VPC 的公网出入口。

云防火墙通过防护 NAT 网关所在的 VPC，实现对 NAT 网关流量的防护。

与企业路由器的关系

企业路由器（Enterprise Router, ER）为云防火墙提供 VPC 间防护的引流能力。当用户购买专业版防火墙，对 VPC 间流量或专线流量进行防护时，企业路由器关联模式需要通过 ER 服务进行引流。

与云监控服务的关系

云监控（Cloud Eye）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。用户可以通过云监控服务的相关指标及时了解云防火墙的防护状况，并根据这些指标调整防护规则。

与云日志服务的关系

云日志服务（Log Tank Service，LTS）用于收集来自主机和云服务的日志数据。云防火墙可以设置将攻击事件日志、访问控制日志、流量日志记录到 LTS 中，为您提供一个实时、高效、安全的日志处理功能。

与 Web 应用防火墙的主要区别

云防火墙和 Web 应用防火墙是两款不同的产品，为您的互联网边界和 VPC 边界、Web 服务提供防护。

CFW 和 WAF 的主要区别说明如表 1-9 所示。

表 1-9 CFW 和 WAF 的主要区别说明

类别	云防火墙	Web 应用防火墙
定义	云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和 VPC 边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持 AI 提升智能防御能力满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	Web 应用防火墙（Web Application Firewall，WAF），通过对 HTTP(S)请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定。

类别	云防火墙	Web 应用防火墙
防护对象	• 弹性公网 IP 和 VPC 边界。 • 支持对 Web 攻击的基础防护。 • 支持外部入侵和主动外联的流量防护。	• 针对域名或 IP，云上或云下的 Web 业务。 • 支持对 Web 攻击的全面防护。
功能特性	• 资产管理与入侵防御：对已开放公网访问的服务资产进行安全盘点，进行实时入侵检测与防御。 • 访问控制：支持互联网边界访问流量的访问控制。 • 流量分析与日志审计：VPC 间流量全局统一访问控制，全流量分析可视化，日志审计与溯源分析。	SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击防护。

1.6 等保合规能力说明

检查项分类	安全控制点	等保合规检查项	风险等级参考	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**	应避免将重要网络区域部署在边界处，重要网络区域与其它网络区域之间应采取可靠的技术隔离手段。	高	通过云原生能力，将重要网络区域隔离，使用云防火墙 CFW 实现业务流量的访问控制，并对恶意访问进行识别和拦截。	1.2 应用场景
		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。	中	通过云防火墙自动识别业务在互联网的威胁暴露面，提供云上互联网边界的防护，入侵防御引擎对恶意流量实时检测和拦截。	
安全区域边界	**边界防护**	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。	高	云防火墙实现南北向访问的网络流量分析、全网流量可视化、对主动外联行为的分析和阻	1.3 产品功能

检查项分类	安全控制点	等保合规检查项	风险等级参考	云防火墙 CFW 提供的对应能力说明	相关功能介绍
		应能够对非授权设备私自连到内部网络的行为进行限制或检查。	中	断、开通或变更白名单策略。	
		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。	中		
	入侵防范	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。	高	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。	
		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。	高	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。	
		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。	中	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。	
	访问控制	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。	高	云防火墙实现统一管理互联网到业务的南北向访问策略和业务，达到协议、端口、应用级访问控制粒度。	《云防火墙用户指南》中《管理访问控制策略》

检查项分类	安全控制点	等保合规检查项	风险等级参考	云防火墙 CFW 提供的对应能力说明	相关功能介绍
		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。	中	云防火墙提供策略命中计数功能，客户可以根据命中情况，及时调整策略的设置，确保没有冗余的策略。云防火墙访问控制策略可配置优先级，您可以根据业务需求优化访问控制列表。	
		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。	高	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。	
		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。	中	云防火墙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。	
		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。	中	云防火墙实现跨流量的应用协议、内容的访问控制。	
	安全审计	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。	高	云防火墙提供日志审计功能，可以记录所有流量日志、事件日志和操作日志。	《云防火墙用户指南》中《日志审计》

检查项分类	安全控制点	等保合规检查项	风险等级参考	云防火墙 CFW 提供的对应能力说明	相关功能介绍
		审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其它与审计相关的信息。	中	云防火墙提供日志记录事件功能，包括：时间、威胁类型、方向、源 IP 和目的 IP、应用类型、严重性等级以及响应动作等信息。	
		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。	中	云防火墙提供日志分析功能，对已分析的日志，默认提供存储 6 个月内的日志数据，并提供实时日志分析能力。	
		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。	中	云防火墙提供日志分析功能，对已分析的日志，默认提供存储 6 个月内的日志数据，并提供实时日志分析能力。	

1.7 术语解释

本文为您介绍云防火墙相关名词的主要含义。

传输控制协议

TCP 是一种面向连接的、可靠的、基于字节流的传输层通信协议，由 IETF 的 RFC 793 定义。

防护流量

入云流量：从 Internet 流入云防火墙方向的流量，例如，从公网下载资源到云内服务器。

出云流量：从云防火墙流出到 Internet 方向的流量，例如，云内服务器对外提供服务，外部用户下载云内的资源。

防护带宽：所有经过云防火墙防护的业务带宽。

互联网边界的流量峰值：所有经过云防火墙防护的 EIP 的流量总和最大值，按照入云流量（入流量）或出云流量（出流量）的最大值取值。

VPC 边界的流量峰值：所有经过云防火墙防护的 VPC 的流量总和最大值。

用户数据报协议

UDP 是一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务，IETF RFC 768 是 UDP 的正式规范。UDP 在 IP 报文的协议号是 17。

弹性公网 IP

弹性公网 IP 可以绑定到用户账户下的任何弹性云服务器上，而不需要是特定的弹性云服务器。与传统静态 IP 地址不同，当弹性云服务器或者区 Region 不可用时，弹性公网 IP 地址可以快速重定向到用户账户下的任何弹性云服务器的公网 IP 地址上。

黑白名单

IP 黑白名单包括 IP 白名单和 IP 黑名单配置，其中 IP 白名单即指定 IP 为可信 IP，源 IP 为可信 IP 的流量不进行攻击检测。IP 黑名单即指定 IP 为恶意 IP，源 IP 为恶意 IP 的流量需要根据检测策略执行相应的动作。

Internet 访问

Internet 访问是指互联网 IP 访问云主机的行为，通过对 Internet 访问防护，可以帮助您及时防御外部入侵。

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。

IP 地址组

IP 地址组是多个 IP 地址的集合，可被防护规则引用，可统一管理具有相同安全要求或需要频繁修改的 IP 地址。通过使用 IP 地址组，可有效应对需要重复多次编辑防护规则的场景，方便管理。

IPS

入侵防御系统（Intrusion Prevention System）。IPS 位于防火墙和网络设备之间。如果检测到攻击，IPS 会在攻击扩散到网络的其它地方之前阻止该恶意通信。

互联网边界防火墙

互联网边界防火墙是一种集群式防火墙，用于检测云资产与互联网之间的通信流量（即南北向流量），支持以弹性 IP 为防护对象的入侵检测防御（IPS）和网络防病毒（AV）功能。

VPC 边界防火墙

VPC 边界防火墙是一种分布式防火墙，用于检测两个 VPC 之间的通信流量（即东西向流量），实现内部业务互访活动的可视化与安全防护。

Inspection VPC

Inspection VPC 是 VPC 边界防火墙中的引流 VPC。用户配置网段后，云防火墙默认创建“Inspection VPC”，在“虚拟私有云”模式中将业务 VPC 的流量引流到防火墙。

1.8 用户权限

系统默认提供两种权限策略：系统策略和自定义策略。系统策略是 IAM 预置的策略，用户只能使用不能修改。如果系统策略不满足授权要求，用户可以创建自定义策略，自由搭配需要授予的权限集。

用户组配置权限策略后，将用户加入用户组中，可以使该用户获得权限策略中定义的操作权限。

2 计费说明

计费项

CFW 包周期（包年/包月）根据您的 CFW 服务版本、购买时长和购买的计费项目计费；按需计费的防火墙按照实际防护情况计费。

表 2-1 计费项信息

服务版本	计费模式	计费项目	计费说明
标准版	包年/包月	购买时长	提供包年和包月的购买模式。
		防护公网 IP 数（可选）	按购买的个数计费。
		防护互联网边界流量峰值（可选）	按购买的流量值计费。
专业版	包年/包月	购买时长	提供包年和包月的购买模式。
		防护公网 IP 数（可选）	按购买的个数计费。
		防护互联网边界流量峰值（可选）	按购买的流量值计费。
		防护 VPC 数（可选）	按购买的个数计费

计费模式

提供包周期（包年/包月）计费模式，购买时长越久越便宜。包周期计费将按照订单的购买周期进行结算。

变更配置

- 变更规格：如果您需要变更 CFW 实例规格，可以先退订当前 CFW 实例后，再重新购买。
- 退订：购买云防火墙后，如需停止使用，请执行退订操作。

续费

包周期购买的版本到期后，您可以单击右上角“续费”，跳转至续费管理页面完成续费，延长使用期。

为避免版本到期未及时续费，导致安全风险，建议开通自动续费。开通自动续费后，系统将根据配置自动续费，无需手动操作。

3 用户指南

3.1 购买及变更云防火墙

3.1.1 购买云防火墙

云防火墙支持一个区域下购买多个防火墙，便于管理不同场景下的资源和策略。

前提条件

使用 IAM 用户时，已授予该 IAM 用户 BSS Administrator 和 CFW FullAccess 权限。

约束条件

- 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。

版本信息说明

云防火墙支持包年/包月（预付费）计费方式，提供以下服务版本：标准版、专业版。

各版本的功能差异请参见 1.3 产品功能。

各服务版本推荐使用的说明如下：

- 标准版

  有等保需求，或对网络入侵、主机失陷等网络安全比较关注的中小型客户。
- 专业版

  有等保或重保需求，或对网络入侵、主机失陷、内部网络互访等网络安全比较关注的中大型客户。

标准版防火墙

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 单击“购买云防火墙”，进入“购买云防火墙”页面，相关参数如表 3-1 所示。

表 3-1 购买标准版防火墙参数说明

参数名称		参数说明
计费模式		包年/包月，按配置周期计费。
区域		购买云防火墙的区域。
版本规格	-	选择版本：标准版。
	扩展防护公网 IP 数	（可选）选择需扩展的防护公网 IP 数，可选择范围：0~2000 个。 **此处为套餐外购买数量**，例如标准版防护公网 IP 数默认 20 个（套餐内费用包含），如果您的公网 IP 是 65 个，那么只需要填写 45 个。
	扩展互联网边界防护带宽	（可选）选择需扩展的防护流量峰值（出流量或入流量的最大峰值），可选择范围：0~5,000Mbps/月（需为 5 的整数倍）。 • **此处为套餐外购买流量值**，例如标准版防护互联网边界流量峰值默认 10Mbps（套餐内费用包含），如果您的防护流量是 200Mbps，那么只需要填写 190Mbps。 • 防护流量按照出流量或入流量的最大峰值取值。
高级设置	防火墙名称	设置当前防火墙的名称。 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）、空格和特殊字符（-_）。 • 长度支持 1-48 个字符。
	企业项目	在下拉列表中选择防火墙归属的企业项目，选择后，防火墙将归属到该企业项目下，用于费用及账单管理；但是，云防火墙的防护层级不会发生改变，仍支持防护所有企业项目下的资源。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。
	标签	（可选）如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在 TMS 中创建预定义标签。

参数名称	参数说明
购买时长	自主选择购买时长。 选择时长后，可勾选“自动续费”若您勾选并同意自动续费，则在服务到期前，系统会自动按照购买周期生成续费订单并进行续费，无需手动续费。

步骤 4 确认信息无误后，单击“立即购买”。

----结束

专业版防火墙

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 单击“购买云防火墙”，进入“购买云防火墙”页面，相关参数如表 3-2 所示。

表 3-2 购买专业版防火墙参数说明

参数名称		参数说明
基础配置	计费模式	包年/包月，按配置周期计费。
	区域	购买云防火墙的区域。
版本规格	-	选择版本：专业版。
	扩展防护公网 IP 数	（可选）选择需扩展的防护公网 IP 数，可选择范围：0~2,000 个。 **此处为套餐外购买数量**，例如专业版防护公网 IP 数默认 50 个（套餐内费用包含），如果您的公网 IP 是 65 个，那么只需要填写 15 个。
	扩展互联网边界防护带宽	（可选）选择需扩展的防护流量峰值（出流量或入流量的最大峰值），可选择范围：0~5,000Mbps/月（需为 5 的整数倍）。 • **此处为套餐外购买流量值**，例如专业版防护互联网边界流量峰值默认 50Mbps（套餐内费用包含），如果您的防护流量是 200Mbps，那么只需要填写 150Mbps。 • 防护流量按照出流量或入流量的最大峰值取值。

参数名称		参数说明
	扩展防护VPC数	（可选）选择需扩展的VPC数，可选择范围：0~100个。 • 仅“专业版”支持VPC间防护功能。 • **此处为套餐外购买数量**，例如专业版防护VPC数默认2个（套餐内费用包含），如果您的VPC是3个，那么只需要填写1个。 • “扩展VPC数”每增加1个，“扩展VPC间防护流量峰值”增加200Mbps。
高级设置	防火墙名称	设置当前防火墙的名称。 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）、空格和特殊字符（-_）。 • 长度支持1-48个字符。
	企业项目	在下拉列表中选择防火墙归属的企业项目，选择后，防火墙将归属到该企业项目下，用于费用及账单管理；但是，云防火墙的防护层级不会发生改变，仍支持防护所有企业项目下的资源。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。
	标签	（可选）如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签。
购买时长		自主选择购买时长。 选择时长后，可勾选“自动续费”若您勾选并同意自动续费，则在服务到期前，系统会自动按照购买周期生成续费订单并进行续费，无需手动续费。

步骤 4 确认信息无误后，单击“立即购买”。

----结束

生效条件

付款成功后，您可以在管理控制台“总览”页面查看当前购买的防火墙版本。

相关文档

- 查看防火墙实例的基本信息、整体防护能力等数据，请参见 3.2 云防火墙防护总览。
- 当前防火墙规格无法满足业务需求，您可以升级防火墙版本或购买扩展包，具体操作请参见 3.1.2 升级云防火墙版本和 3.1.3 变更云防火墙扩展包数量。

3.1.2 升级云防火墙版本

购买了云防火墙后，如果当前版本功能无法满足您的需求，您可以升级 CFW 的版本。

从标准版升级到专业版

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在页面左上角，单击“升级到专业版”，进入升级云防火墙页面。

步骤 5 确认版本规格后，单击“立即购买”。

----结束

生效条件

付款成功后，您可以在管理控制台“总览”页面查看当前购买的防火墙版本。

相关文档

- 4.4.3 如何为云防火墙续费？
- 4.4.4 如何退订云防火墙？

3.1.3 变更云防火墙扩展包数量

购买了云防火墙后，您可以增加或减少 EIP/VPC 的防护数量以及互联网边界流量峰值。

变更扩展包

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在“防火墙详情”中，单击“已使用/可防护 EIP 数”、“已使用/可防护 VPC 数”、“互联网边界防护带宽”右侧的“变更”，进入“变更云防火墙规格”页面。

步骤 5 变更扩展包数量。

默认不支持将扩展包数量降到 0，如果您需要将扩展包数量降到 0，请参见退订扩展包。

----结束

退订扩展包

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 鼠标悬停在页面左上角上角版本处，单击“退订”。

步骤 5 选择退订的扩展包，单击“确认”。

步骤 6 确认信息无误后，勾选“我已确认本次退订金额和相关费用。”

步骤 7 单击“下一步”，完成退订操作。

----结束

3.2 云防火墙防护总览

您可以在总览页面查看防火墙实例的基本信息、整体防护能力、统计信息、流量拓扑可视化信息，随时了解云资产的安全状况以及流量数据。

约束条件

VPC 边界防护详情需配置 3.3.2 开启 VPC 边界流量防护后才能查看。

查看总览

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换或查看防火墙实例：

- 切换防火墙实例：在页面左上角的下拉框中切换防火墙。
- 查看防火墙实例信息：单击右上角“防火墙列表”，参数说明请参见表 3-3。

表 3-3 防火墙实例信息

参数名称	参数说明
防火墙名称/ID	防火墙的名称/ID。
状态	防火墙的运行状态。

参数名称	参数说明
版本	防火墙的版本规格。
可防护 EIP 数	当前防火墙最大可防护的 EIP 数量。
可防护互联网流量峰值	当前防火墙最大可防护流量的峰值。
计费模式	当前防火墙的计费模式。
企业项目	防火墙所属的企业项目。
操作	支持查看详情操作。

步骤 4 在总览页面，可以查看以下几个板块信息：

- 资源概况
- 安全事件
- 防护规则
- 运营看板
- 防火墙详情

----结束

资源概况

展示当前账号的当前区域下所有云资源（EIP、VPC）的防护状态（未防护数及总数）。

安全事件

展示入侵防御功能的防护总详情，可快速定位需要防护的云资产。

- 在右上角切换查询时间，支持查询 5 分钟~7 天的数据。

防护规则

查看防护策略的未命中数量和总数。

详细的未命中防护策略，可单击“一个月以上未命中策略数”的数字，跳转在“策略助手”页面，底部列表中查看。

运营看板

- 切换“互联网边界”和“VPC 边界”，查看对应场景云资源总体防护数据。
- 在右上角切换查询时间，支持查询 5 分钟~7 天的数据。
- **出/入方向流量峰值、出/入方向 95 带宽、访问控制拦截：**

  查看访问控制策略的拦截效果，以及出/入方向流量的 95 带宽和最大值。取值说明如表 3-4 所示。

表 3-4 出/入方向流量峰值、出/入方向 95 带宽、访问控制拦截取值说明

时间段	取值
近 1 小时	取 1 分钟内的最大值。
近 24 小时	取 5 分钟内的最大值。
近 7 天	取 1 小时内的最大值。
自定义	• 5 分钟~6 小时：取 1 分钟内的最大值。 • 6 小时（含）~3 天：取 5 分钟内的最大值。 • 3 天（含）~7 天（含）：取 30 分钟内的最大值。

- 流量峰值：系统每个周期统计 1 个带宽值，某段时间内统计的最大值即流量峰值。

  例如：出方向流量峰值为 100bps，则在某段时间（例如 24 小时）内，带宽的最大值为 100bps。
- 95 带宽：系统每个周期统计 1 个带宽值，将某段时间内的带宽值进行降序排列，去掉带宽数值最高的前 5%的值，剩余的最高带宽即为 95 带宽。

  例如：出方向 95 带宽为 100bps，则在某段时间（例如 24 小时）内，带宽值经过降序排列并去掉最高的 5%的值后，剩余的最高带宽为 100bps。

- **流量趋势：**

  查看出/入方向和整体的流量变化趋势，可在右上角选择待查看弹性公网 IP、以及“平均值”或“最大值”。取值说明如表 3-5 所示。

表 3-5 流量趋势取值说明

时间段	平均值	最大值
近 1 小时	取 1 分钟内的平均值。	取 1 分钟内的最大值。
近 24 小时	取 5 分钟内的平均值。	取 5 分钟内的最大值。
近 7 天	取 1 小时内的平均值。	取 1 小时内的最大值。
自定义	• 5 分钟~6 小时：取 1 分钟内的平均值。 • 6 小时（含）~3 天：取 5 分钟内的平均值。 • 3 天（含）~7 天（含）：取 30 分钟内的平均值。	• 5 分钟~6 小时：取 1 分钟内的最大值。 • 6 小时（含）~3 天：取 5 分钟内的最大值 • 3 天（含）~7 天（含）：取 30 分钟内的最大值。
注：基于流量统计数据，数据信息实时更新。		

- **攻击趋势**：查看入侵防御功能拦截或放行的防护情况，修改入侵防御配置请参见 3.5.2 配置入侵防御。
- **访问控制**：查看访问控制策略阻断或放行的防护情况，修改访问控制策略请参见 3.4 访问控制。

防火墙详情

在页面右侧，“防火墙详情”中展示当前防火墙实例详细信息，参数说明如表 3-6 所示。

表 3-6 防火墙实例详细信息

参数名称		参数说明
基本信息	版本	防火墙的版本规格，支持“标准版”和“专业版”。
	防火墙名称	当前防火墙实例的名称，支持单击 修改名称。
	防火墙 ID	当前防火墙实例的 ID。
	状态	当前防火墙的状态。开通或退订防火墙大约需要 5 分钟更新状态。
	企业项目	当前防火墙所属的企业项目。
规格	已使用/可防护 EIP 数	当前防火墙实例已开启防护的弹性公网 IP 数量/可防护的弹性公网 IP 总数。
	已使用/可防护 VPC 数	当前防火墙实例已开启防护的 VPC 数量/可防护的 VPC 总数。
	互联网边界防护带宽	所有经过云防火墙防护的 EIP 的流量总和最大值，按照入云流量（入流量）或出云流量（出流量）的最大值取值。
	VPC 边界防护带宽	可防护的东西向流量峰值。 所有经过云防火墙防护的 VPC 的流量总和最大值。
	已使用/可使用防护规则	当前防火墙实例已创建的防护规则数量/可创建的防护规则总数。
交易信息	计费模式	购买的计费模式。
标签		用于标识防火墙，方便您对防火墙进行分类。

3.3 云防火墙防护

3.3.1 开启互联网边界流量防护

云防火墙通过对弹性公网 IP（EIP）的防护实现互联网边界流量的防护，开启 EIP 防护后，您的业务流量将经过云防火墙，默认情况下，所有流量都会被放行。

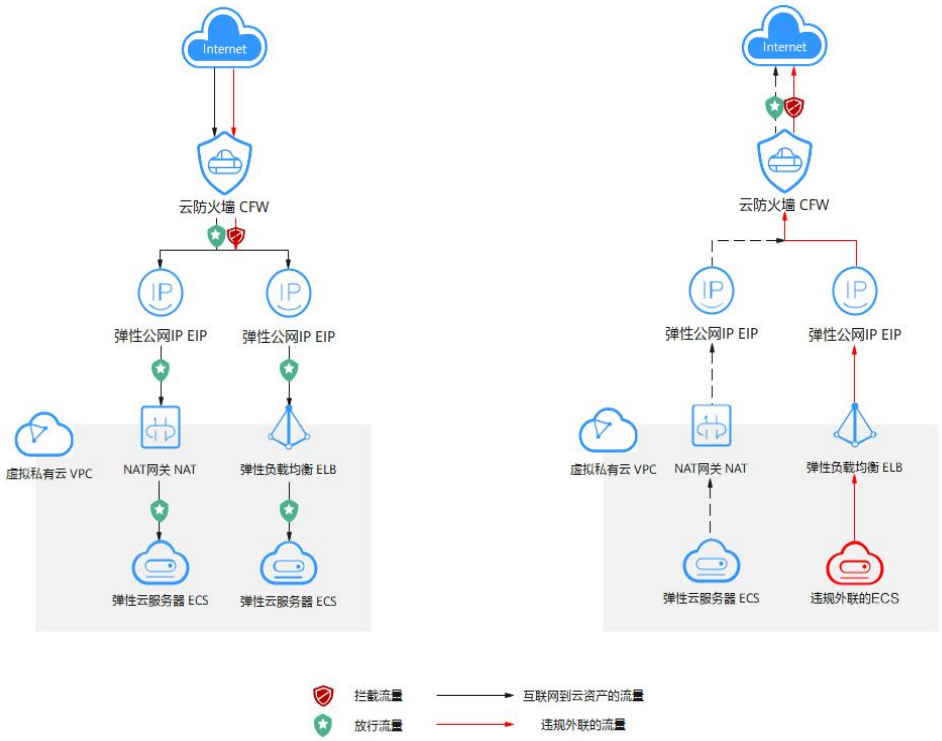
开启防护后，您可以根据业务需求，配置访问控制策略或 IPS 防护模式，云防火墙会根据具体配置，检测流量实施拦截/放行操作。

配置访问控制策略详细操作请参见 3.4.2.1 通过防护规则拦截/放行流量，IPS 相关详细介绍及操作请参见 3.5.2 配置入侵防御。

什么是互联网边界流量

互联网边界流量是云资产（包括 IPv4 和 IPv6）与互联网之间的通信流量（即南北向流量），分为入云流量（互联网访问云资产）和出云流量（云资产主动访问互联网）。

图 3-2 互联网边界流量防护



约束条件

- 一个 EIP 只能在一个防火墙上开启防护。

对业务的影响

开启 EIP 防护前，请确认是否有阻断所有流量的防护规则或黑名单：

- 开启 EIP 防护前，如果有阻断所有流量的防护规则或黑名单，则会在开启时对该 EIP 生效，可能导致业务中断。此时，建议在开启防护前排查是否存在长连接且不支持会话重建的业务。如果存在，请先进行处理。

  编辑防护规则详细操作请参见 3.4.4.3 管理防护规则。编辑黑名单详细操作请请参见 3.4.4.4 管理黑白名单。
- 开启或关闭 EIP 防护前，如果不存在阻断所有流量的防护规则或黑名单，则不会造成业务中断，保证流量平滑切换。

开启互联网边界流量防护

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 > 弹性公网 IP 管理”，进入“弹性公网 IP 管理”页面，弹性公网 IP（包括 IPv4 和 IPv6）信息将自动更新至列表中。

步骤 5 开启弹性公网 IP。

一个 EIP 只能在一个防火墙上开启防护。

- 开启单个弹性公网 IP：在所在行的“操作”列中，单击“开启防护”。
- 开启多个弹性公网 IP：勾选需要开启防护的弹性公网 IP，单击列表上方的“开启防护”。

步骤 6 在弹出的界面确认信息无误后，单击“绑定并开启防护”，可查看操作行的“防护状态”列显示“防护中”。

EIP 开启防护后，系统默认放行所有流量，即访问控制策略默认动作为“放行”。

----结束

新增 EIP 自动防护

开启新增 EIP 自动防护后，CFW 会在整点自动同步 EIP 资源并对新增的 EIP 开启防护，EIP 流量将被防火墙防护。

开启方式：进入 CFW 的“弹性公网 IP 管理”页面，在页面上方开启“新增 EIP 自动防护”开关。

后续操作

- 查看经过云防火墙的流量趋势和统计结果，请参见 3.6 流量分析，详细流量记录请参见流量日志。
- 开启防护后，流量默认放行，云防火墙将根据您设置的策略实施拦截：

表 3-7 设置策略

目标动作	操作指导
如果希望实现流量管控	可通过配置防护策略来进行处理，具体说明如下： • 通过防护规则放行/拦截流量： – 添加放行的防护规则：放行后的流量会经过入侵防御IPS、病毒防御等功能的检测。 – 添加拦截的防护规则：流量将直接拦截。 • 通过黑白名单放行/拦截流量： – 添加白名单：流量将直接放行，不再经过其他功能的检测。 – 添加黑名单：流量将直接拦截。 详细操作请参见 3.4.2.1 通过防护规则拦截/放行流量或 3.4.2.5 通过黑白名单拦截/放行流量。
如果希望拦截网络攻击	可通过配置入侵防御来进行处理，详细操作请参见 3.5.2 配置入侵防御。

相关操作

- 关闭弹性公网 IP 防护：

⚠ 注意

关闭弹性公网 IP（EIP）防护后，CFW 将不再防护该 EIP 的流量，可能会导致该 EIP 遭受恶意攻击，**请谨慎操作**。

  - 关闭单个弹性公网 IP。在所在行的“操作”列中，单击“关闭防护”。
  - 关闭多个弹性公网 IP。勾选需要开启防护的弹性公网 IP，单击表格上方的“关闭防护”。
- 导出弹性公网 IP 列表信息：在列表上方，单击“导出”，根据数据范围选择选项。

3.3.2 开启 VPC 边界流量防护

3.3.2.1 VPC 边界防火墙概述

云防火墙支持防护虚拟私有云（VPC）的流量，开启防护后，您的业务流量将经过云防火墙，默认情况下，所有流量都会被放行。

配置访问控制策略详细操作请参见 3.4.2.1 通过防护规则拦截/放行流量，IPS 相关详细介绍及操作请参见 3.5.2 配置入侵防御。

本文介绍云防火墙中 VPC 边界防火墙的相关概念和防护配置。

什么是 VPC 边界流量

VPC 边界流量是 VPC 与线下数据中心 IDC、VPC 与 VPC 之间的通信流量（即东西向流量），您可以通过云防火墙配置 VPC 边界防火墙，借助企业路由器，实现内部业务互访活动的可视化与安全防护。

VPC 边界防火墙支持跨账号防护功能。例如，A 账号下有 VPC_A，B 账号下有 VPC_B，您只需在 A 账号中配置企业路由器和云防火墙，将 A 账号的企业路由器共享至 B 账号，并添加 VPC_B 的连接，即可防护 A、B 两个账号下的 VPC 资源。

图 3-3 VPC 与 IDC 之间

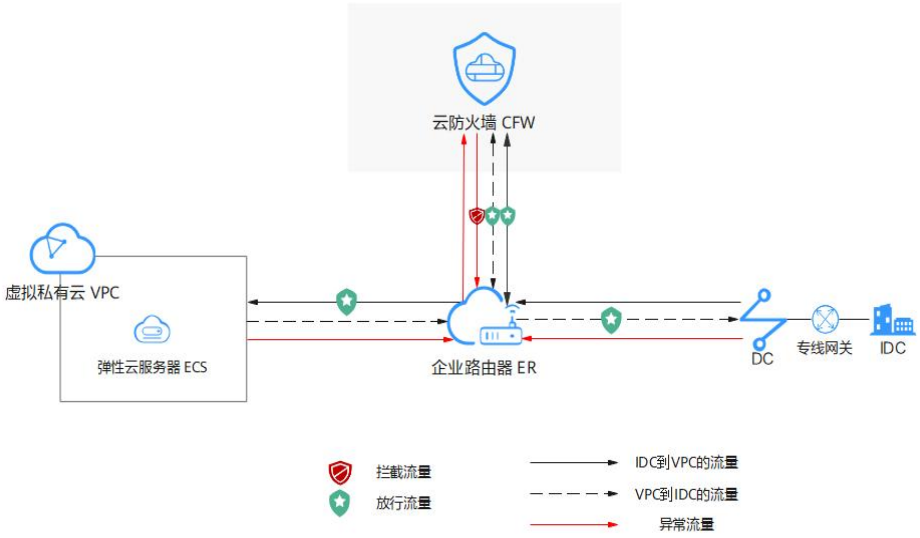
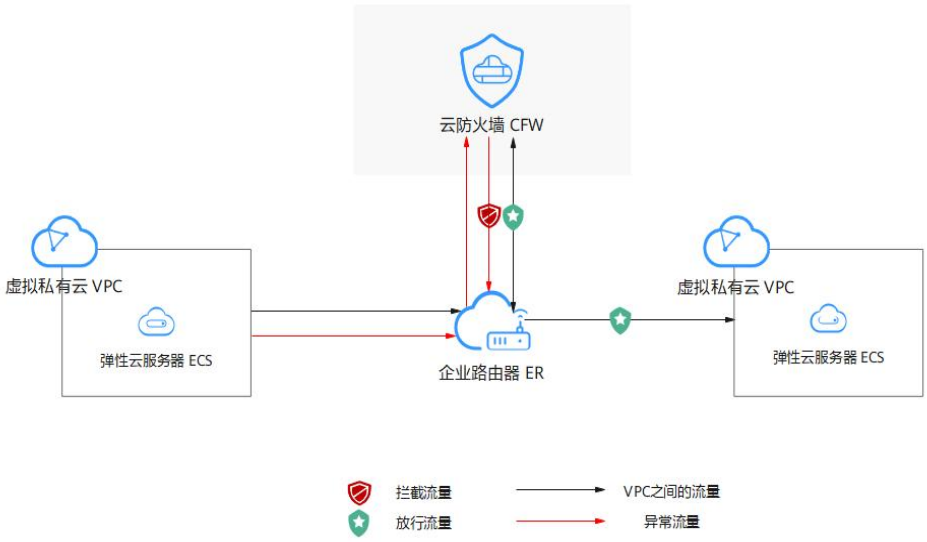


图 3-4 VPC 与 VPC 之间



支持的防护对象

- 虚拟私有云（VPC）
- 虚拟网关（VGW）
- 虚拟专用网络（VPN）
- 全域接入网关（DGW）

约束条件

- 仅“专业版”支持 VPC 边界防火墙。
- 依赖企业路由器（Enterprise Router，ER）服务引流。

对业务的影响

开启 VPC 防护前，请确认是否有阻断所有流量的防护规则或黑名单：

- 开启 VPC 防护前，如果有阻断所有流量的防护规则或黑名单，则会在开启时对该 VPC 生效，可能导致业务中断。此时，建议开启防护前排查是否存在长连接且不支持会话重建的业务。如果存在，请先进行处理。

  编辑防护规则详细操作请参见 3.4.4.3 管理防护规则。编辑黑名单详细操作请参见 3.4.4.4 管理黑白名单。
- 开启或关闭 VPC 防护前，如果不存在阻断所有流量的防护规则或黑名单，则不会造成业务中断，保证流量平滑切换。

配置流程

表 3-8 企业路由器模式（新版）配置及使用流程

操作步骤	操作说明
3.3.2.2.1 创建 VPC 边界防火墙	为 VPC 边界防火墙规划用于引流的网段。 说明 引流 VPC 不会创建在您的账号上，即不占用您的防护 VPC 个数。
3.3.2.2.2 配置企业路由器并将流量引至云防火墙	通过企业路由器连通 VPC 和云防火墙之间的流量。 • 为防护 VPC 添加连接，建立 VPC 与 ER 之间的网络互通。 • 在企业路由器中创建两个路由表作为关联路由表和传播路由表，将 VPC 和防火墙之间的流量互相传输。 • 为 VPC 添加一条指向企业路由器的路由。
3.3.2.2.3 开启/关闭 VPC 边界防火墙并确认流量经过云防火墙	开启 VPC 边界流量防护，并验证流量是否经过云防火墙。
VPC 边界防护规则	通过防护规则放行/拦截流量（放行后的流量会经过入侵防御 IPS、病毒防御等功能的检测）。
3.4.2.5 通过黑白名单拦截/放行流量	通过黑白名单放行/拦截流量（放行/拦截的流量，不再经过其它功能的检测）。
访问控制日志	查看防护策略是否生效。

图 3-4 为虚拟私有云关联模式的配置流程：

图 3-5 虚拟私有云关联模式配置流程

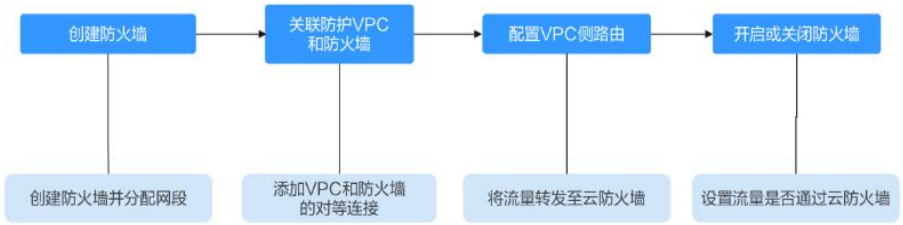
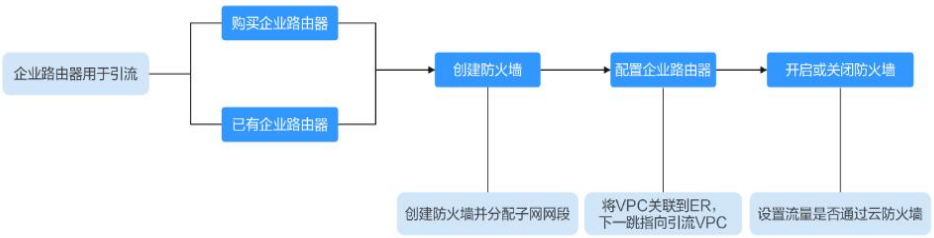


图 3-5 为企业路由器模式关联模式（旧版）的配置流程：

图 3-6 企业路由器关联模式配置流程



3.3.2.2 企业路由器模式（新版）

3.3.2.2.1 创建 VPC 边界防火墙

VPC 边界防火墙能够检测和统计 VPC 间的通信流量数据，帮助您发现异常流量。开启 VPC 边界防火墙之前，您需要先创建 VPC 边界防火墙并关联企业路由器。

前提条件

当前账号下需存在可用的企业路由器（企业路由器限制）。

- 关于企业路由器的收费，请参见《企业路由器用户指南 > 计费说明》。
- 创建企业路由器请参见《企业路由器用户指南 > 创建企业路由器》。
  创建时，建议取消勾选“默认路由表关联”和“默认路由表传播”。

约束条件

仅“专业版”支持 VPC 边界防火墙。

创建说明

创建防火墙时为了引流需选择企业路由器和配置 IPV4 网段。

- 企业路由器用于引流，选择时需满足以下限制：
  - 没有与其它防火墙实例关联。
  - 需归属本账号，非共享企业路由器。
  - 需关闭“默认路由表关联”、“默认路由表传播”和“自动接收共享连接”功能。
- 网段用于将流量转发至云防火墙，选择时需注意以下限制：
  - 该网段不可与需要开启防护的私网网段重合，否则会导致路由冲突。
  - 10.6.0.0/16-10.7.0.0/16 网段为防火墙保留网段，不可使用。

创建 VPC 边界防火墙

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

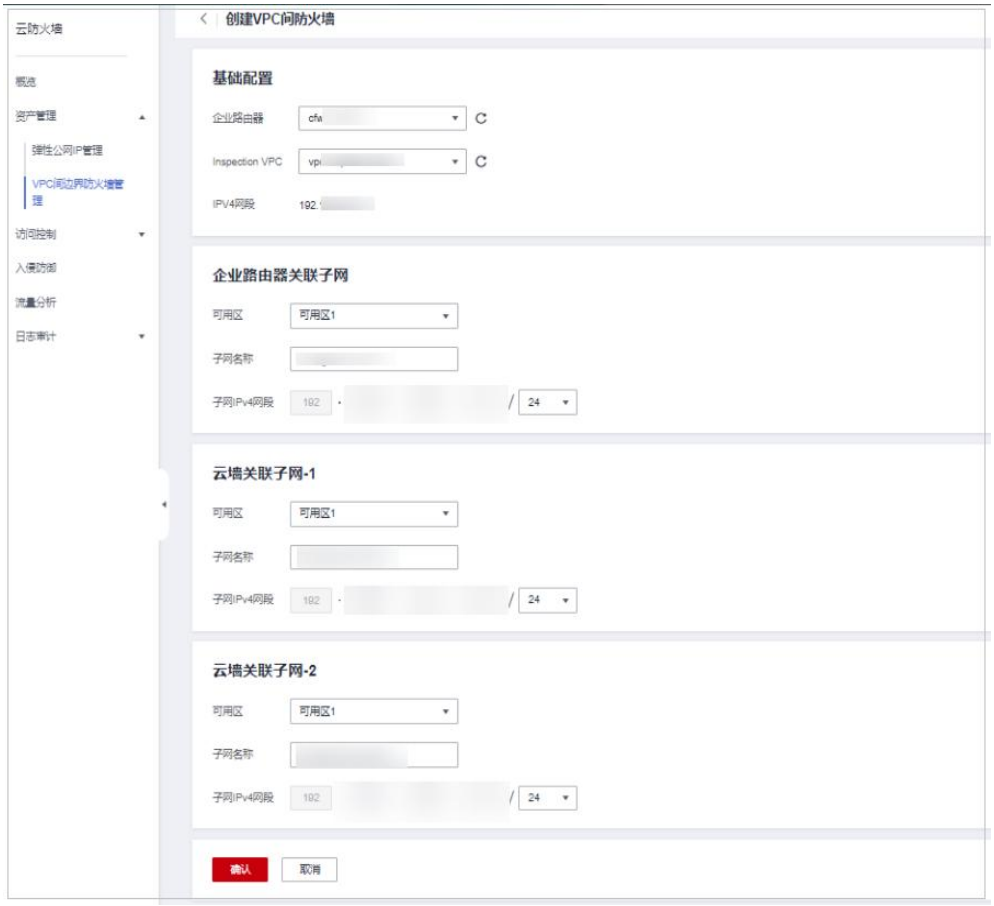
步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 单击“创建防火墙”。

步骤 6 选择企业路由器并配置合适的网段。

- 企业路由器用于引流，选择时需满足以下限制：
  - 没有与其它防火墙实例关联。
  - 需归属本账号，非共享企业路由器。
  - 需关闭“默认路由表关联”、“默认路由表传播”和“自动接收共享连接”功能。
- 网段配置后默认创建 InspectionVPC 将流量转发至云防火墙，并自动分配云墙关联子网，将云防火墙流量转发到企业路由器，选择时需注意以下限制：
  - 创建防火墙后不支持修改网段。
  - 该网段需满足以下条件：
    - 仅支持私网地址段（即在 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 范围中），否则可能在 SNAT 等访问公网的场景下产生路由冲突。
    - 10.6.0.0/16-10.7.0.0/16 网段为防火墙保留网段，不可使用。
    - 不可与需要开启防护的私网网段重合，否则会因路由冲突，导致该网段无法防护。
- 如果您参数界面如图 3-6 所示，则您目前云防火墙版本为旧版，VPC 边界防火墙配置请参见 3.3.2.3 企业路由器模式（旧版）。

图 3-7 创建 VPC 边界防火墙



步骤 7 单击“确认”，需等待 3-5 分钟，完成防火墙创建。

创建过程中您只能浏览“总览”页，防火墙的“状态”会变为“升级中”。

----结束

相关文档

关闭防火墙：防火墙创建后不支持删除和退订，您可以关闭防火墙的防护请参见关闭 VPC 边界防火墙。

3.3.2.2.2 配置企业路由器并将流量引至云防火墙

本文指导您通过企业路由器将流量引至云防火墙，并验证网络的连通性。

前提条件

流量互通，确定流量未经过防火墙时正常通信。流量验证请参见《企业路由器用户指南 > 验证网络互通情况》。

配置原理和流程

配置企业路由器时的流量走势如图 3-7 所示，操作流程如图 3-8 所示。

图 3-8 流量走势图

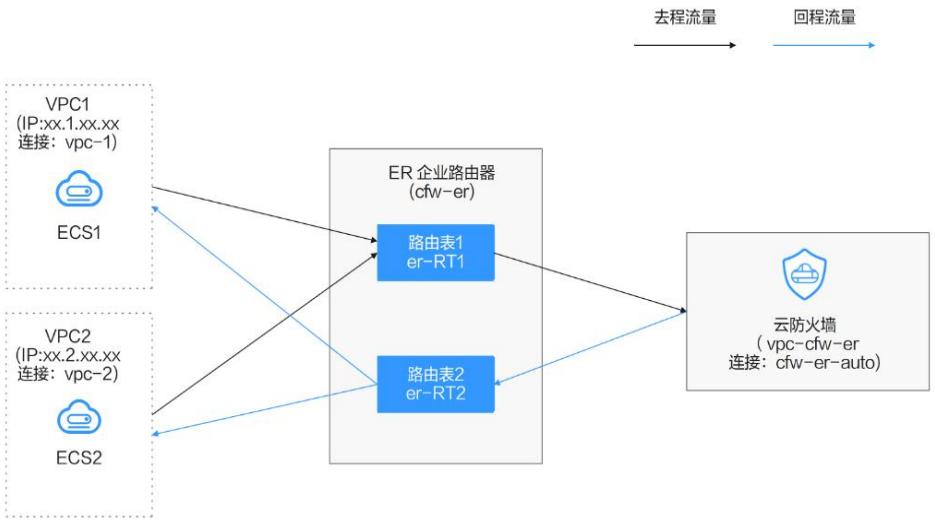
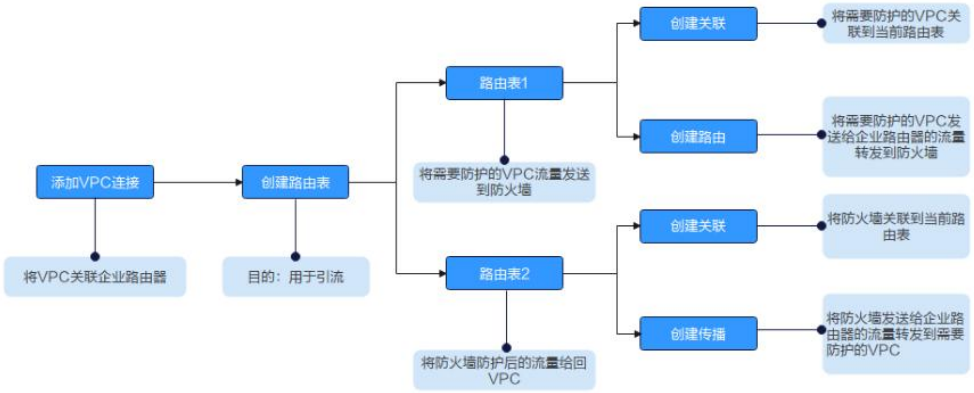


图 3-9 操作流程



通过配置企业路由器将流量引至云防火墙

步骤 1 创建 VPC 边界防火墙，具体操作请参见 3.3.2.2.1 创建 VPC 边界防火墙。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 添加 VPC 连接。

单击“防火墙状态”侧的“编辑防护 VPC”，进入企业路由器页面，在企业路由器中添加连接，支持添加的连接类型请参见《企业路由器用户指南》中“连接概述”章节。

下文以防护两个 VPC 为例（至少需要添加两条 VPC 连接，用于连接两个 VPC 和 ER 之间）。操作步骤请参见《企业路由器用户指南 > 在企业路由器中添加 VPC 连接》。

图 3-10 添加 VPC 连接

说明

- 防火墙创建后自动生成一条防火墙连接（名称：cfw-er-auto-attach，连接类型：云防火墙（CFW）），防护 VPC 的连接需手动添加；每增加一个防护的 VPC，都需要增加一条连接。

  例如：对 VPC1 连接命名为 vpc-1；对 VPC2 连接命名为 vpc-2，需防护 VPC3 时，增加连接命名为 vpc-3。
- 如需防护其它账号（如账号 B）下的 VPC，请将当前账号 A 的企业路由器共享至账号 B，共享步骤请参见《企业路由器用户指南 > 创建共享》，共享成功后在账号 B 中添加连接，后续配置仍在账号 A 中进行。

步骤 6 创建两个路由表，作为**关联路由表**和**传播路由表**分别用于连接需防护的 VPC 和连接防火墙。

单击“路由表”页签，进入路由表设置页面，单击“创建路由表”，参数详情见表 3-9。

表 3-9 创建路由表参数说明

参数名称	参数说明
名称	输入路由表的名称。 命名规则如下： • 长度范围为 1~64 位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。

参数名称	参数说明
描述	您可以根据需要在文本框中输入对该路由表的描述信息。
标签	您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。

步骤 7 配置关联路由表。

1. 设置关联功能：在路由表设置页面，选择关联路由表，单击“关联”页签，单击“创建关联”，参数详情见表 3-10。

   关联至少需要添加两条，每增加一个防护的 VPC，都需增加一条关联。

   例如：选择 VPC1 的连接 vpc-1 以及 VPC2 的连接 vpc-2，需防护 VPC3 时，增加一条关联，选择连接 vpc-3。

表 3-10 创建关联参数说明

参数名称	参数说明
连接类型	选择连接类型“虚拟私有云（VPC）”。
连接	在连接下拉列表中，选择需防护的 VPC 连接。

2. 设置路由功能：单击“路由”页签，单击“创建路由”，根据实际数量创建路由功能，参数详情见表 3-11。

表 3-11 创建路由参数说明

参数名称	参数说明
目的地址	设置目的地址。 • 0.0.0.0/0：VPC 的所有流量（IPv4）都会经过云防火墙防护。 • 网段：该网段的流量会经过云防火墙防护。
黑洞路由	建议您保持关闭状态；开启后如果路由匹配上黑洞路由的目的地址，则该路由的报文会被丢弃。
连接类型	选择连接类型“虚拟私有云（VPC）”。
下一跳	在下拉列表中，选择自动生成的防火墙连接（cfw-er-auto-attach）。
描述	（可选）路由的描述信息。

步骤 8 配置传播路由表。

1. 设置关联功能：在路由表设置页面，选择传播路由表，单击“关联”页签，单击“创建关联”，参数详情见表 3-12。

表 3-12 创建关联参数说明

参数名称	参数说明
连接类型	选择连接类型“虚拟私有云（VPC）”。
连接	在下拉列表中，选择自动生成的防火墙连接（cfw-er-auto-attach）。

2. 设置传播功能：单击“传播”页签，单击“创建传播”，参数详情见表 3-13。

表 3-13 创建传播参数说明

参数名称	参数说明
连接类型	选择连接类型“虚拟私有云（VPC）”。
连接	在传播下拉列表中，选择需防护的 VPC 连接。

说明

- 传播至少需要添加两条，每增加一个防护的 VPC，都需增加一条传播。

  例如：选择 VPC1 的连接 vpc-1 以及 VPC2 的连接 vpc-2，需防护 VPC3 时，增加一条传播，选择连接 vpc-3。
- 创建传播后，会自动将连接的路由信息学习到 ER 路由表中，生成“传播路由”。同一个路由表中，不同传播路由的目的地址可能相同，连接配置不支持修改和删除。
- 您也可以手动在路由表中配置连接的静态路由，同一个路由表中，静态路由的目的地址不允许重复，连接配置支持修改和删除。
- 如果路由表中存在多条路由目的地址相同，则优先级：静态路由 > 传播路由。

步骤 9 修改 VPC 的路由表。

1. 在左侧导航栏中，选择“网络 > 虚拟私有云 > 路由表”，进入“路由表”页面。
2. 在“名称/ID”列，单击对应 VPC 的路由表名称，进入路由表“基本信息”页面。
3. 单击“添加路由”，参数详情见表 3-14。

   至少需要为两个 VPC 添加路由，每增加一个防护的 VPC，都需为该 VPC 增加一条路由。

表 3-14 添加路由参数说明

参数	说明
目的地址类型	选择“IP 地址”。

参数	说明
目的地址	流量到达的网段，且填写的网段不能与已有路由和 VPC 下子网网段冲突。 例如两个 VPC 间防护时，VPC1 中添加的路由“目的地址”填写 VPC2 的网段。
下一跳类型	在下拉列表中，选择类型“企业路由器”。
下一跳	选择下一跳资源。 下拉列表中将展示您创建的企业路由器名称。
描述	（可选）路由的描述信息。 描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。

4. 单击“确定”。

----结束

修改已有企业路由器将流量引至云防火墙

步骤 1 已创建 VPC 边界防火墙，具体操作请参见 3.3.2.2.1 创建 VPC 边界防火墙。

步骤 2 登录管理控制台。

步骤 3 在左侧导航栏中，单击左上方的 ☰，选择“网络 > 企业路由器”，进入“企业路由器”页面。

步骤 4 从默认路由表 er-RT1 中删除防火墙 VPC(vpc-cfw-er)的关联和传播。

选择“路由表 > 关联”，在防火墙 VPC 行的“操作”列，单击“删除”，在删除确认框中，单击“是”。

选择“传播”，在防火墙 VPC 行的“操作”列，单击“删除”，在删除确认框中，单击“是”。

步骤 5 创建路由表 er-RT2。

单击页面左上角“创建路由表”。参数详情见表 3-15。

表 3-15 创建路由表参数说明

参数名称	参数说明	取值样例
名称	输入路由表的名称。要求如下： • 长度范围为 1~64 位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	er-RT2

参数名称	参数说明	取值样例
标签	您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。	“标签键”：test “标签值”：01
描述	您可以根据需要在文本框中输入对该路由表的描述信息。	-

步骤 6 配置路由表 er-RT2：设置关联和传播功能。

1. 选择路由表 er-RT2，单击“关联”页签，单击“创建关联”。参数详情见表 3-16 。

表 3-16 创建关联参数说明

参数名称	参数说明	取值样例
连接类型	选择连接类型“云防火墙（CFW）”。	云防火墙（CFW）
连接	在连接下拉列表中，选择防火墙 VPC 的连接。	cfw-er-auto

2. 创建同一路由表(er-RT2)的传播功能。单击“传播”页签，单击“创建传播”。参数详情见表 3-17。

表 3-17 创建传播参数说明

参数名称	参数说明	取值样例
连接类型	选择连接类型“虚拟私有云（VPC）”。	虚拟私有云（VPC）
连接	在传播下拉列表中，选择需防护的 VPC 连接。	vpc-1

表 3-18 创建传播参数说明

参数名称	参数说明	取值样例
连接类型	选择连接类型“虚拟私有云（VPC）”。	虚拟私有云（VPC）
连接	在传播下拉列表中，选择需防护的 VPC 连接。	vpc-2

说明

- 传播至少需要添加两条，每增加一个防护的 VPC，都需增加一条传播。

  例如：选择 VPC1 的连接 vpc-1 以及 VPC2 的连接 vpc-2，需防护 VPC3 时，增加一条传播，选择连接 vpc-3。
- 创建传播后，会自动将连接的路由信息学习到 ER 路由表中，生成“传播路由”。同一个路由表中，不同传播路由的目的地址可能相同，连接配置不支持修改和删除。
- 您也可以手动在路由表中配置连接的静态路由，同一个路由表中，静态路由的目的地址不允许重复，连接配置支持修改和删除。
- 如果路由表中存在多条路由目的地址相同，则优先级：静态路由 > 传播路由。

步骤 7 配置默认路由表 er-RT1：

1. 添加静态路由。选择路由表 er-RT1，单击“路由”页签，单击“创建路由”，填写信息如下：
   - 目的地址：0.0.0.0/0
   - 连接类型：“云防火墙（CFW）”
   - 下一跳：选择防火墙 VPC 的连接（cfw-er-auto）
2. 删除路由表 er-RT1 中的**所有**传播。

   单击“传播”页签，在“操作”列中，单击“删除”，在删除确认框中，单击“是”。

步骤 8（可选）建议您将当前企业路由器的传播路由表改为新创建的路由表（er-RT2），后续添加新 VPC 时，仅需添加连接，无需进行其它操作。

返回或进入“企业路由器”，单击“更多 > 修改配置”，选择传播路由表为 er-RT2。如图 3-10 所示。

图 3-11 修改配置

如需防护其它账号（如账号 B）下的 VPC，请将当前账号 A 的企业路由器共享至账号 B，共享步骤请参见《企业路由器用户指南 > 创建共享》，共享成功后在账号 B 中添加连接即可完成配置。

----结束

后续操作

配置后开启 VPC 边界防护，请参见 3.3.2.2.3 开启/关闭 VPC 边界防火墙并确认流量经过云防火墙。

3.3.2.2.3 开启/关闭 VPC 边界防火墙并确认流量经过云防火墙

配置完成后，防火墙默认为“未开启”状态，此时流量只经过企业路由器，未转发到防火墙。您可选择手动开启或关闭 VPC 边界防火墙功能。

开启 VPC 边界防火墙

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 在“防火墙状态”侧，单击“开启防护”。

步骤 6 单击“确认”，完成开启 VPC 边界防火墙。

----结束

关闭 VPC 边界防火墙

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 在“防火墙状态”侧，单击“关闭防护”。

步骤 6 单击“确认”，完成关闭 VPC 边界防火墙。关闭后，您 VPC 边界的流量将不会被防火墙防护。

----结束

验证流量是否经过云防火墙

步骤 1 生成流量，请参见《企业路由器用户指南 > 验证网络互通情况》。

步骤 2 查看日志：在左侧导航栏中，选择“日志审计 > 日志查询”，选择“流量日志 > VPC 边界防火墙”页签。

- 有日志记录：云防火墙已成功防护 VPC 间流量。
- 无日志记录，排查企业路由器配置，请参见 3.3.2.2.2 配置企业路由器并将流量引至云防火墙。

----结束

3.3.2.3 企业路由器模式（旧版）

3.3.2.3.1 购买企业路由器

企业路由器（Enterprise Router, ER）可以连接 VPC 或本地网络来构建中心辐射型组网，是云上大规格，高带宽，高性能的集中路由器。

前提条件

关于企业路由器的收费，请参见《企业路由器计费说明》。

约束条件

仅专业版支持 VPC 间防火墙防护功能。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 单击“购买企业路由器”，进入“企业路由器”控制台，购买步骤请参见《企业路由器用户指南》中《创建企业路由器》。

说明

建议您取消开启“默认路由表关联”、“默认路由表传播”和“自动接收共享连接”功能，后文会指导您配置路由表。

----结束

3.3.2.3.2 创建 VPC 边界防火墙

VPC 边界防火墙能够检测和统计 VPC 间的通信流量数据，帮助您发现异常流量。开启 VPC 边界防火墙之前，您需要先创建 VPC 边界防火墙。

前提条件

- 已有企业路由器。
- 创建 VPC 边界防火墙需使用您防护 VPC 配额中的一个 VPC 作为 Inspection VPC 用于引流，所以当前账号需存在一个无流量且未规划子网的 VPC，并满足账号下 VPC 可创建路由表的配额不小于 2。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 配置企业路由器关联子网和云墙关联子网。单击“创建防火墙”，进入“创建 VPC 间防火墙”页面，配置企业路由器和关联子网信息。

图 3-12 创建 VPC 边界防火墙

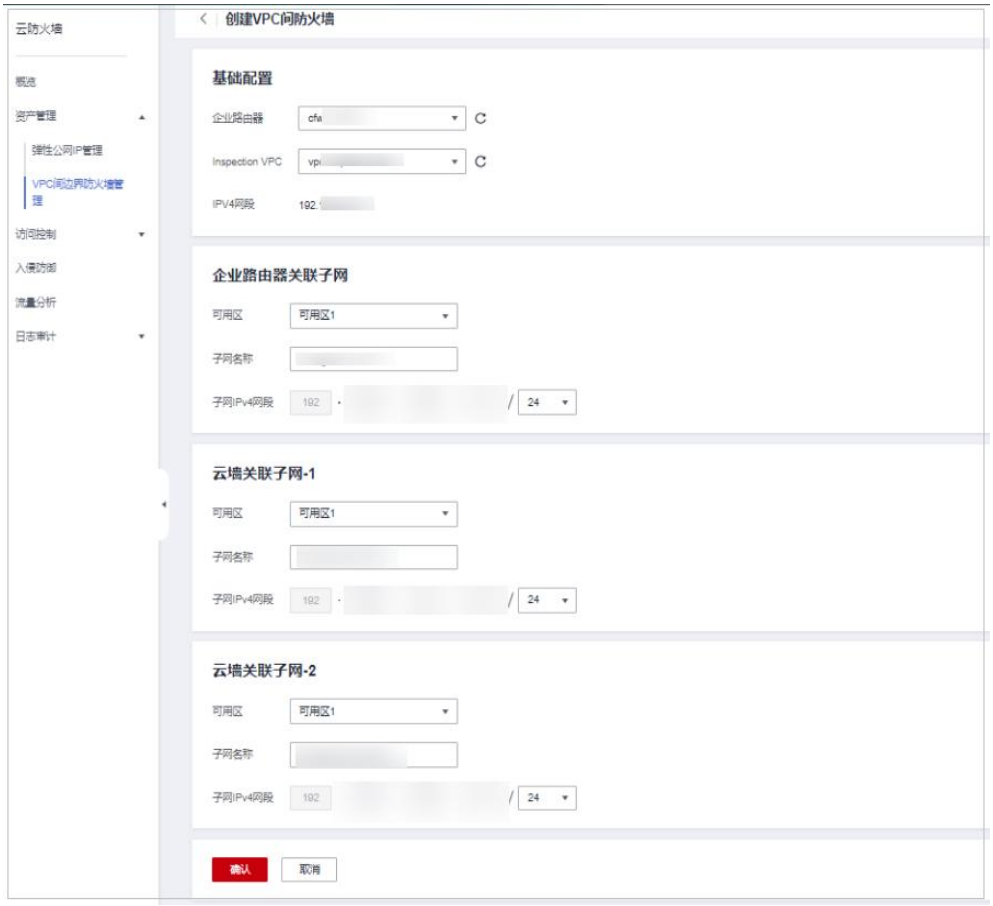


表 3-19 创建 VPC 边界防火墙参数说明

参数名称	参数说明	取值示例
企业路由器	选择您的企业路由器。	cfw-er
Inspection VPC	选择 VPC。此处的 Inspection VPC 不能与用于关联企业路由器的其他 VPC 有重叠网段。	vpc-cfw-er
IPV4 网段	选择 VPC 后自动出现 IPV4 地址。	xx.xx.0.0/16
可用区	选择可用区。	可用区 1
子网名称(企业路由器关联子网）	自定义子网名称。	cfw-er-1
子网名称(云墙关联子网-1）		cfw-er-2

参数名称	参数说明	取值示例
子网名称 (云墙关联子网-2）		cfw-er-3
子网 IPV4 网段 (企业路由器关联子网）	分配子网 IPV4 网段。 说明 • 需跟现有子网不冲突。 • 三个子网网段之间不冲突。	xx.xx.1.0/24
子网 IPV4 网段（云墙关联子网-1）		xx.xx.2.0/24
子网 IPV4 网段 (云墙关联子网-2）		xx.xx.3.0/24

步骤 6 单击“确认”，需等待 3-5 分钟，完成防火墙创建。

创建过程中您只能浏览“概览”页，防火墙的“状态”会变为“升级中”。

----结束

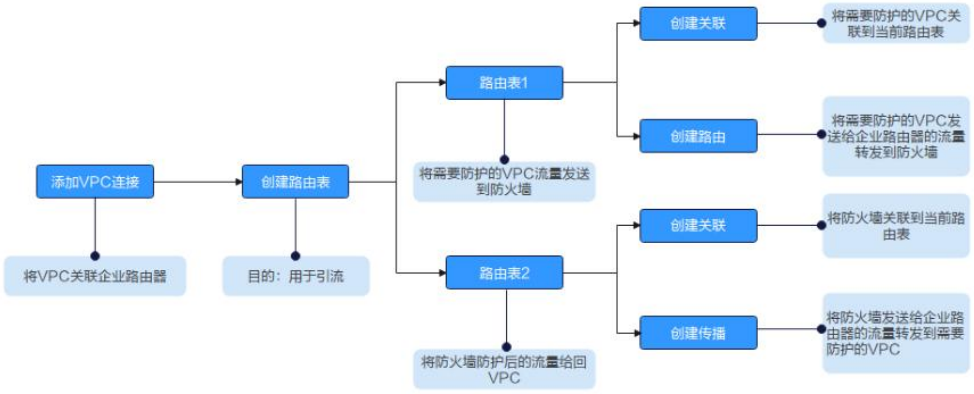
3.3.2.3.3 配置企业路由器

防火墙创建完成后，您还需关联企业路由器和设置引流。

配置原理

配置企业路由器时需要执行以下流程。

图 3-13 配置企业路由器操作步骤



前提条件

已完成创建防火墙步骤。

约束条件

- 企业路由器需关闭“默认路由表关联”、“默认路由表传播”和“自动接收共享连接”功能。
- 仅专业版支持 VPC 间防火墙防护功能。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 单击“配置企业路由器”，进入“企业路由器”页面，在企业路由器中添加连接，支持添加的连接类型请参见《企业路由器用户指南》中《连接概述》。

下文以防护两个 VPC 为例（至少需要添加两条 VPC 连接，用于连接两个 VPC 和 ER 之间）。操作步骤请参见《企业路由器用户指南》中《在企业路由器中添加 VPC 连接》。

说明

- 连接至少需要添加三条，例如：对防火墙连接命名为 cfw-er-auto（创建防火墙后自动生成）；对 VPC1 连接命名为 vpc-1；对 VPC2 连接命名为 vpc-2。
- 如需防护其他账号（如账号 B）下的 VPC，请将当前账号 A 的企业路由器共享至账号 B，共享步骤请参见《企业路由器用户指南》中《创建共享》，共享成功后在账号 B 中添加连接，后续配置仍在账号 A 中进行。

步骤 6 创建两个路由表分别用于连接需防护的 VPC 和连接防火墙。

单击“路由表”页签，进入路由表设置页面，单击“创建路由表”。

参数详情见表 3-20。

表 3-20 创建路由表参数说明

参数名称	参数说明	取值样例
名称	输入路由表的名称。 命名规则如下： • 长度范围为 1~64 位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	er-rlb-4cd1
描述	您可以根据需要在文本框中输入对该路由表的描述信息。	-
标签	您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。	-

步骤 7 设置关联和路由功能。

1. 在路由表设置页面，选择用于连接需防护 VPC 的路由表，单击“关联”页签，单击“创建关联”。

   参数详情见表 3-21。

表 3-21 创建关联参数说明

参数名称	参数说明	取值样例
连接类型	选择连接类型“虚拟私有云（VPC）”。	虚拟私有云（VPC）
连接	在连接下拉列表中，选择需防护的 VPC 连接。	er-attach-01

2. 创建同一路由表的路由功能。单击“路由”页签，单击“创建路由”，根据实际数量创建路由功能。

   参数详情见表 3-22。

表 3-22 创建路由参数说明

参数名称	参数说明	取值样例

参数名称	参数说明	取值样例
目的地址	设置目的地址。 可以是虚拟私有云网段、子网网段。 说明 若您的 ECS 绑定公网 EIP，配置路由时需指定网段，不能使用 0.0.0.0/0。	192.168.2.0/24
连接类型	选择连接类型“虚拟私有云（VPC）”。	虚拟私有云（VPC）
下一跳	在下一跳下拉列表中，选择防火墙的 VPC 连接。	er-Inspection

步骤 8 设置关联和传播功能。

1. 在路由表设置页面，单击“关联”页签，选择用于连接防火墙的路由表，单击“创建关联”。

   参数详情见表 3-23 。

表 3-23 创建关联参数说明

参数名称	参数说明	取值样例
连接类型	选择连接类型“虚拟私有云（VPC）”。	虚拟私有云（VPC）
关联	在连接下拉列表中，选择防火墙 VPC 的连接。	er-Inspection

2. 创建同一路由表的传播功能。单击“传播”页签，单击“创建传播”。

   参数详情见表 3-24。

表 3-24 创建传播参数说明

参数名称	参数说明	取值样例
连接类型	选择连接类型“虚拟私有云（VPC）”。	虚拟私有云（VPC）
传播	在传播下拉列表中，选择需防护的 VPC 连接。	er-attach-02

说明

- 创建传播后，会自动将连接的路由信息学习到 ER 路由表中，生成“传播路由”。同一个路由表中，不同传播路由的目的地址可能相同，连接配置不支持修改和删除。

- 您也可以手动在路由表中配置连接的静态路由，同一个路由表中，静态路由的目的地址不允许重复，连接配置支持修改和删除。
- 如果路由表中存在多条路由目的地址相同，则优先级：静态路由 > 传播路由。

----结束

配置验证方法

前提条件

- 已完成全部配置步骤。
- 两个 VPC 中各有一台 ECS。

验证方式

VPC 中的 ECS 互相 *ping*，确定流量未经过防火墙时是否正常通信。

故障定位

步骤 1 企业路由器的两个路由表配置是否正确。正确配置方式请参见步骤 7 和步骤 8。

步骤 2 检查待防护 VPC 的默认路由表是否将路由转向企业路由器。

查看方式：

1、在左侧导航栏中，选择“网络 > 虚拟私有云 > 路由表”，进入“路由表”页面，在“名称/ID”列，单击对应 VPC 的路由表名称。

2、查看是否存在“下一跳类型”为“企业路由器”的路由。若不存在，单击“添加路由”，参数详情见表 3-25。

表 3-25 添加路由参数说明

参数	说明	取值样例
目的地址	目的地址网段。 目的地址不能与已有路由冲突，目的地址也不能与 VPC 下子网网段冲突。 **说明** 不能与已有路由和 VPC 下子网网段冲突。	192.168.0.0/16
下一跳类型	在下拉列表中，选择类型“企业路由器”。	企业路由器
下一跳	选择下一跳资源。 下拉列表中包含资源将基于您所选的资源类型进行展示。	er-01

参数	说明	取值样例
描述	路由的描述信息，非必填项。 说明 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

----结束

3.3.2.3.4 开启/关闭 VPC 间边界防火墙

配置完成后，防火墙默认为“未开启”状态，此时流量只经过企业路由器，未转发到防火墙。您可选择手动开启或关闭 VPC 间防火墙功能。

前提条件

- 已购买 CFW 专业版。
- 已配置企业路由器。

约束条件

- 仅专业版支持 VPC 间防火墙防护功能。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 在“操作”列，单击“开启防护”或“关闭防护”。

----结束

3.3.2.4 管理 VPC 边界防火墙

3.3.2.4.1 新增防护 VPC

操作场景

当您完成 VPC 边界防火墙配置后，需要配置路由等将流量转发给云防火墙。

本章节介绍如何快速配置、修改路由。

前提条件

已配置完成 VPC 边界防火墙，具体操作请参见 3.3.2.2 企业路由器模式（新版）。

步骤一：添加 VPC 连接

操作步骤请参见《企业路由器用户指南 > 在企业路由器中添加 VPC 连接》。

如需防护其它账号（如账号 B）下的 VPC，请将当前账号 A 的企业路由器共享至账号 B，共享步骤请参见《企业路由器用户指南 > 创建共享》，共享成功后在账号 B 中添加连接，后续配置仍在账号 A 中进行。

步骤二：配置关联路由表的关联和传播路由表的传播

步骤 1 在左侧导航栏中，单击左上方的 ☰，选择“网络 > 企业路由器”，单击“管理路由表”，进入“路由表”页面。

步骤 2 设置关联功能：在路由表设置页面，选择关联路由表，单击“关联”页签，单击“创建关联”，参数详情见表 3-26。

关联至少需要添加两条，每增加一个防护的 VPC，都需增加一条关联。

例如：选择 VPC1 的连接 vpc-1 以及 VPC2 的连接 vpc-2，需防护 VPC3 时，增加一条关联，选择连接 vpc-3。

表 3-26 创建关联参数说明

参数名称	参数说明
连接类型	选择连接类型“虚拟私有云（VPC）”。
连接	在连接下拉列表中，选择需防护的 VPC 连接。

步骤 3 设置传播功能：选择传播路由表，单击“传播”页签，单击“创建传播”，参数详情见表 3-27。

表 3-27 创建传播参数说明

参数名称	参数说明
连接类型	选择连接类型“虚拟私有云（VPC）”。
连接	在传播下拉列表中，选择需防护的 VPC 连接。

说明

- 传播至少需要添加两条，每增加一个防护的 VPC，都需增加一条传播。

例如：选择 VPC1 的连接 vpc-1 以及 VPC2 的连接 vpc-2，需防护 VPC3 时，增加一条传播，选择连接 vpc-3。

- 创建传播后，会自动将连接的路由信息学习到 ER 路由表中，生成“传播路由”。同一个路由表中，不同传播路由的目的地址可能相同，连接配置不支持修改和删除。
- 您也可以手动在路由表中配置连接的静态路由，同一个路由表中，静态路由的目的地址不允许重复，连接配置支持修改和删除。
- 如果路由表中存在多条路由目的地址相同，则优先级：静态路由 > 传播路由。

----结束

步骤三：修改 VPC 的路由表

步骤 1 在左侧导航栏中，选择“网络 > 虚拟私有云 > 路由表”，进入“路由表”页面。

步骤 2 在“名称/ID”列，单击对应 VPC 的路由表名称，进入路由表“基本信息”页面。

步骤 3 单击“添加路由”，参数详情见表 3-28。

至少需要为两个 VPC 添加路由，每增加一个防护的 VPC，都需为该 VPC 增加一条路由。

表 3-28 添加路由参数说明

参数	说明
目的地址类型	选择“IP 地址”。
目的地址	流量到达的网段，且填写的网段不能与已有路由和 VPC 下子网网段冲突。 例如两个 VPC 间防护时，VPC1 中添加的路由“目的地址”填写 VPC2 的网段。
下一跳类型	在下拉列表中，选择类型“企业路由器”。
下一跳	选择下一跳资源。 下拉列表中将展示您创建的企业路由器名称。
描述	（可选）路由的描述信息。 描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。

步骤 4 单击“确定”。

----结束

相关操作

- VPC 边界防火墙介绍，请参见 3.3.2.1 VPC 边界防火墙概述。
- 配置 VPC 边界防火墙操作，请参见 3.3.2.2 企业路由器模式（新版）。

3.3.2.4.2 修改私网网段地址

如果您存在私用公网（即使用 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 以及运营商级 NAT 保留网段 100.64.0.0/10 以外的公网网段作为私网地址段）的情况，请您修改私网网段，否则云防火墙可能无法正常转发 VPC 间的流量。

修改私网网段

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。

步骤 5 在“自定义私网地址段”侧，单击“编辑私网地址段”。

步骤 6 在弹框中修改私网地址。

步骤 7 单击“确认”，完成添加。

----结束

3.3.2.4.3 关闭 VPC 边界防护

如果业务遇到异常拦截，可以暂时关闭 VPC 边界防火墙，关闭期间，防火墙对流量不做任何检测。

对业务的影响

关闭后，VPC 边界的流量将不会被防火墙防护，需谨慎操作。

3.3.2.4.4 永久关闭 VPC 边界防护后恢复企业路由器配置

如果业务后续不再需要 VPC 边界流量防护，在 3.3.2.4.3 关闭 VPC 边界防护后，需要手动恢复企业路由器（ER）的配置。

本节指导您恢复 ER 的配置，恢复后，流量将直接从 VPC1 --> ER --> VPC2，不再经过云防火墙。

⚠ 警告

关闭 VPC 防护并恢复企业路由器配置后，CFW 将不再防护 VPC 间的流量，请谨慎操作。

应用场景

当前业务不再需要 VPC 边界防火墙防护。

恢复企业路由器配置

步骤 1 关闭 VPC 边界防火墙防护，请参见 3.3.2.4.3 关闭 VPC 边界防护。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“网络 > 企业路由器”，单击“管理路由表”，进入“路由表”页面。

步骤 3 将传播路由表中的路由（配置传播后自动生成）配置到关联路由表中。

1. 在“关联路由表”的“路由”页签中，单击“创建路由”。参数信息填写“传播路由表”的“路由”配置中防护 VPC 的“目的地址”和“下一跳”。
   - 关联路由表：将流量从 VPC 传输到云防火墙的路由表，配置时的操作请参见配置关联路由表。

     传播路由表：将流量从云防火墙传输到 VPC，配置时的操作请参见配置传播路由表。
   - 在“关联路由表”中添加的路由条数需和“传播路由表”中展示的路由条数相同。
2. （可选）删除“传播路由表”。

说明

本步骤仅做提醒，如果不删除传播路由表，不影响流量从 VPC1 --> ER --> VPC2。

----结束

3.3.3 开启 NAT 网关流量防护

操作场景

当 VPC 内的资源（如 ECS）通过 NAT 网关访问互联网时，可能存在未授权访问、数据泄露或恶意攻击等安全风险。为应对这些风险，云防火墙提供业务 VPC 与 NAT 网关之间流量的防护，能够有效阻断非法外联和恶意流量，并支持基于私网 IP 实现细粒度访问控制，拦截未授权的流量访问。

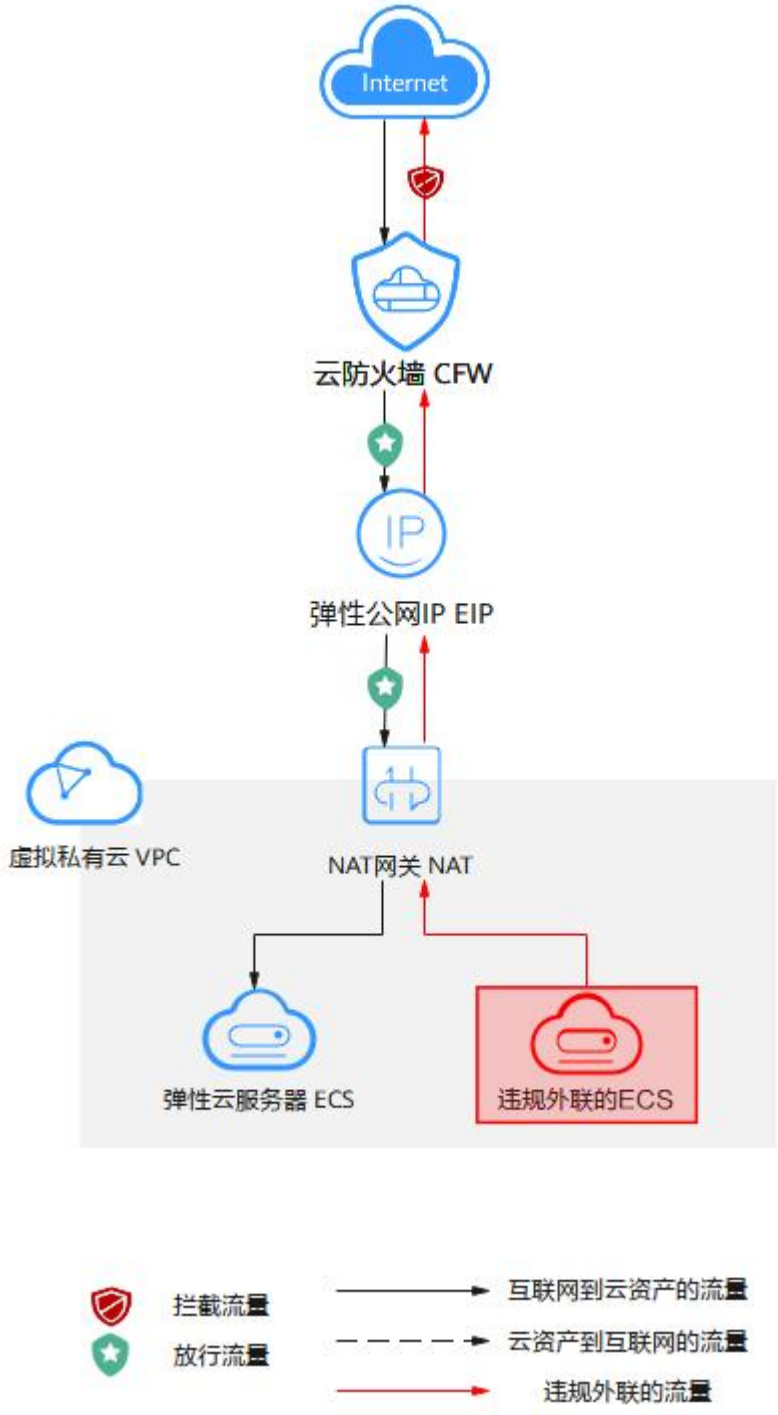
本章节介绍如何通过 VPC 边界防火墙对 NAT 网关流量开启防护，如果业务流量通过 EIP 连接公网请参见 3.3.1 开启互联网边界流量防护。

什么是 NAT 网关流量

NAT 网关流量是 NAT 网关和互联网之间的通信流量，分为两种防护场景：

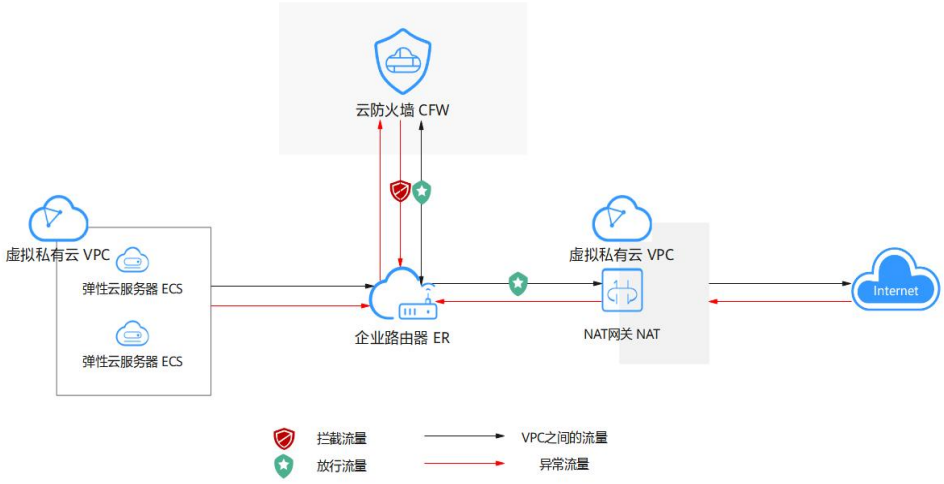
- 通过 NAT 网关绑定的弹性公网 IP（EIP）连接公网，云防火墙会防护所有经过 NAT 网关的流量，适用于防护粒度较粗的场景。

图 3-14 通过 EIP 防护 NAT 网关



- 创建 VPC 边界防火墙，借助企业路由器（ER），接入 NAT 网关所在的 VPC 与业务 VPC 之间，能够防护私网 IP 的流量。

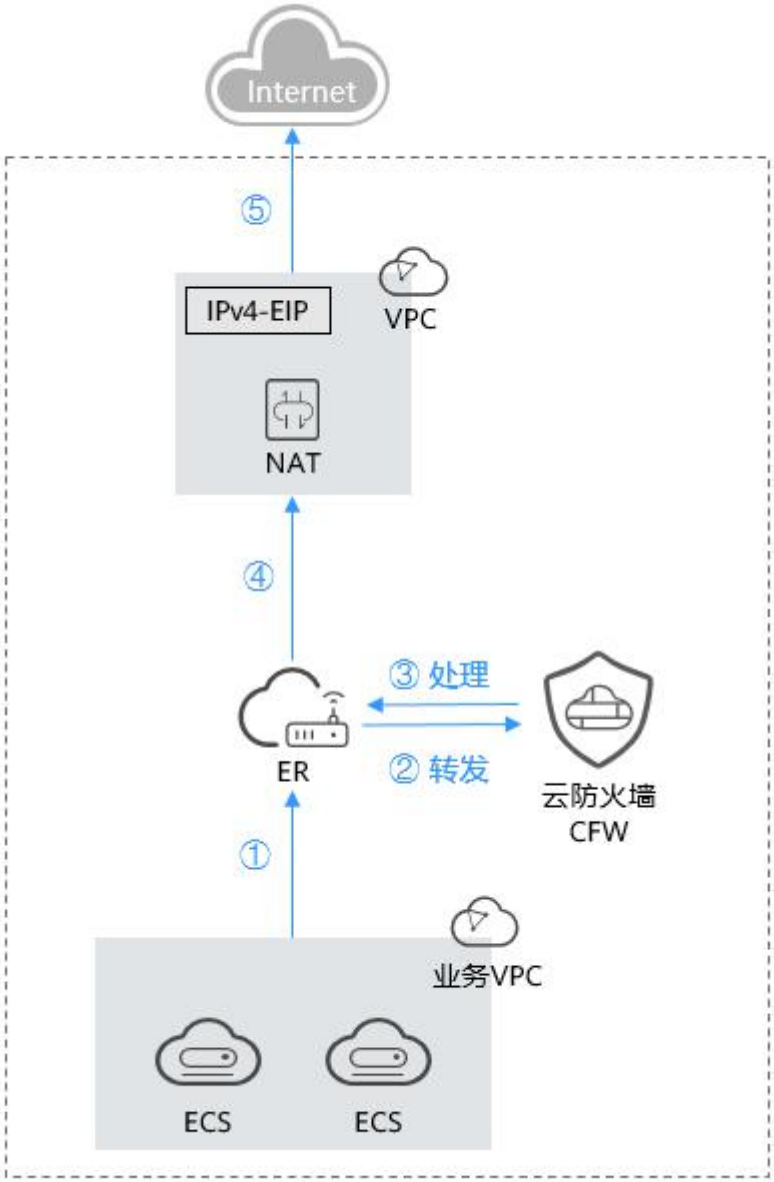
图 3-15 通过 VPC 防护 NAT 网关



SNAT 组网图

SNAT 防护提供主动外联场景的细粒度访问控制，适用于 NAT 网关所在 VPC 与业务 VPC 隔离，并通过多个 VPC/子网使用公网 IP 对外发起访问的场景。

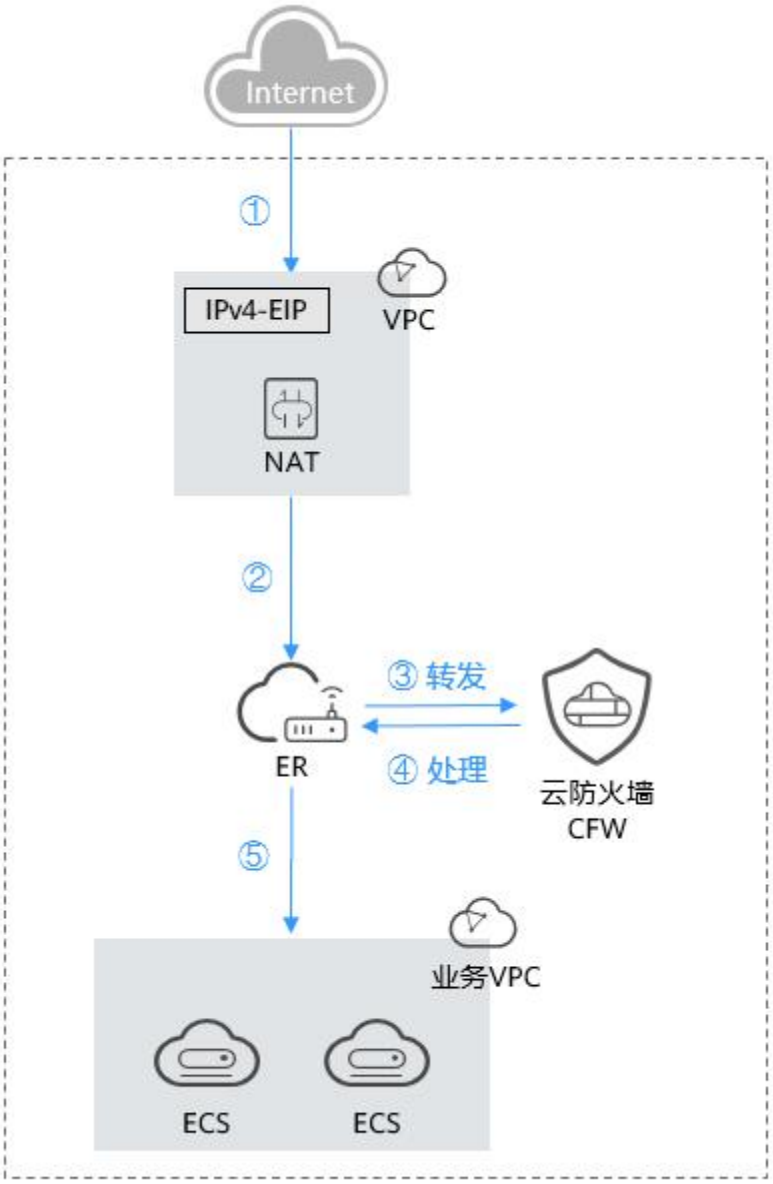
当弹性云服务器（ECS）发起外网访问时，流量经过企业路由器（ER）转发到防火墙，防火墙根据配置的 SNAT 防护规则筛选流量（阻断\放行），将安全的流量放行至 ER，转发到 NAT 网关，通过 SNAT 规则转发到互联网。



DNAT 组网图

DNAT 防护提供外网访问内部资源场景的细粒度访问控制，适用于 NAT 网关所在 VPC 与业务 VPC 隔离，多个 VPC/子网使用 NAT 对外提供访问的场景。

当互联网发起对内部资源的访问时，流量经过 NAT 网关的 DNAT 规则转发到企业路由器（ER），ER 将流量转发至防火墙，防火墙根据配置的 SNAT 防护规则筛选流量（阻断\放行），将安全的流量放行至 ER，转发到业务 VPC。



对业务的影响

开启 VPC 防护前，请确认是否有阻断所有流量的防护规则或黑名单：

- 开启 VPC 防护前，如果有阻断所有流量的防护规则或黑名单，则会在开启时对该 VPC 生效，可能导致业务中断。此时，建议开启防护前排查是否存在长连接且不支持会话重建的业务。如果存在，请先进行处理。

  编辑防护规则详细操作请参见 3.4.4.3 管理防护规则。编辑黑名单详细操作请参见 3.4.4.4 管理黑白名单。
- 开启或关闭 VPC 防护前，如果不存在阻断所有流量的防护规则或黑名单，则不会造成业务中断，保证流量平滑切换。

约束条件

- 仅“专业版”支持 NAT 网关流量防护。
- 依赖企业路由器（Enterprise Router，ER）服务引流。
- 云防火墙当前默认支持标准私网网段，如果您需要配置其它的网段，请您 3.3.2.4.2 修改私网网段地址，否则云防火墙可能无法正常转发您 VPC 间的流量。
- 如要实现 DNAT 网关向 CFW 集群东西向引流并配置 DNAT 规则，需提工单联系服务运维人员支撑防火墙升级，避免因旧版本不支持 DNAT 可能引起的流量受损风险。

开启 NAT 网关流量防护

需完成创建防火墙，具体配置请参见 3.3.2.2.1 创建 VPC 边界防火墙。

步骤一：将 VPC1 和 VPC-NAT 接入企业路由器中

1. 添加 VPC 连接。

   操作步骤请参见《企业路由器用户指南 > 在企业路由器中添加 VPC 连接》。

   说明

   连接需要添加两条，“连接资源”分别选择 VPC1 和 VPC-NAT。

2. 创建两个路由表。

   a. 在左侧导航栏中，单击左上方的 ☰，选择“网络 > 企业路由器”，单击“管理路由表”，进入“路由表”页面。

   b. 创建两个路由表，作为**关联路由表**和**传播路由表**分别用于连接需防护的 VPC 和连接防火墙。

      单击“路由表”页签，进入路由表设置页面，单击“创建路由表”，参数详情见表 3-29。

表 3-29 创建路由表参数说明

参数名称	参数说明
名称	输入路由表的名称。 命名规则如下： • 长度范围为 1~64 位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。
描述	您可以根据需要在文本框中输入对该路由表的描述信息。
标签	您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。

3. 设置关联路由表。

   a. 设置关联功能，添加 VPC1 和 VPC-NAT 的连接：在路由表设置页面，选择关联路由表，单击“关联”页签，单击“创建关联”，参数详情见表 3-30。

      需要增加两条关联，“连接”分别选择 VPC1 和 VPC-NAT 的连接。

表 3-30 创建关联参数说明

参数名称	参数说明
连接类型	选择连接类型“虚拟私有云（VPC）”。
连接	在连接下拉列表中，选择 VPC 连接。

   b. 添加静态路由，指向防火墙：单击“路由”页签，单击“创建路由”，参数详情见表 3-31。

表 3-31 创建路由参数说明

参数名称	参数说明
目的地址	设置目的地址。 • 0.0.0.0/0：VPC 的所有流量（IPv4）都会经过云防火墙防护。 • 网段：该网段的流量会经过云防火墙防护。
黑洞路由	建议您保持关闭状态；开启后如果路由匹配上黑洞路由的目的地址，则该路由的报文会被丢弃。
连接类型	选择连接类型“虚拟私有云（VPC）”。
下一跳	在下拉列表中，选择自动生成的防火墙连接（cfw-er-auto-attach）。
描述	（可选）路由的描述信息。

4. 设置传播路由表。

   a. 设置传播功能，添加 VPC1 的传播：在路由表设置页面，选择传播路由表，单击“传播”页签，单击“创建传播”，参数详情见表 3-32。

表 3-32 创建传播参数说明

参数名称	参数说明
连接类型	选择连接类型“虚拟私有云（VPC）”。
连接	在传播下拉列表中，选择 VPC1 的连接。

b. 添加静态路由，指向 VPC-NAT：单击“路由”页签，单击“创建路由”，参数详情见表 3-33。

表 3-33 创建路由参数说明

参数名称	参数说明
目的地址	设置目的地址，设置为：0.0.0.0/0。
黑洞路由	建议保持关闭状态；开启后如果路由匹配上黑洞路由的目的地址，则该路由的报文会被丢弃。
连接类型	选择连接类型“虚拟私有云（VPC）”。
下一跳	在下拉列表中，选择 VPC-NAT 的连接。

步骤二：配置 NAT 网关

1. 配置 SNAT 规则。
   a. 返回至企业路由器界面，在左侧导航栏中，选择“网络 ＞NAT 网关”，进入“公网 NAT 网关”页面。
   b. 单击公网 NAT 网关的名称，进入“基本信息”页面，切换至“SNAT 规则”页签。
   c. 单击“添加 SNAT 规则”，参数详情如表 3-34 所示。

表 3-34 添加 SNAT 规则

参数名称	参数说明
使用场景	SNAT 规则使用的场景，选择“虚拟私有云”。
网段	选择“自定义”子网，使云服务器通过 SNAT 方式访问公网 • 自定义：自定义一个网段或者填写某个 VPC 的地址。
弹性公网 IP	用来提供互联网访问的公网 IP。 这里只能选择没有被绑定的弹性公网 IP，或者被绑定在当前公网 NAT 网关中非“所有端口”类型 DNAT 规则上的弹性公网 IP，或者被绑定到当前公网 NAT 网关中 SNAT 规则上的弹性公网 IP。 可选择多条 EIP 添加在 SNAT 规则中。一条 SNAT 规则最多添加 20 个 EIP。SNAT 规则使用多个 EIP 时，业务运行时会随机选取其中的一个。
监控	为 SNAT 连接数设置告警。 可通过设置告警及时了解 SNAT 连接数运行状况，从而起到预警作用。
描述	SNAT 规则信息描述。最大支持 255 个字符。

2. 配置是 VPC-NAT 的路由表。
   a. 在左侧导航栏中，选择“网络 > 虚拟私有云 > 路由表”，进入“路由表”页面。
   b. 在“名称”列，单击 NAT 网关对应 VPC 的路由表名称，进入路由表“基本信息”页面。
   c. 单击“添加路由”，参数详情见表 3-35。

表 3-35 添加路由参数说明

参数	说明
目的地址类型	选择“IP 地址”。
目的地址	目的地址网段，填写 VPC1 的 IP 地址。 填写的网段不能与已有路由和 VPC 下子网网段冲突。
下一跳类型	在下拉列表中，选择类型“企业路由器”。
下一跳	选择下一跳资源。 下拉列表中将展示您创建的企业路由器名称。
描述	路由的描述信息，非必填项。 描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。

步骤三：配置 VPC1 路由表

1. 在“路由表”页面的“名称”列，单击 VPC1 的路由表名称，进入路由表“基本信息”页面。
2. 单击“添加路由”，参数详情见表 3-36。

表 3-36 添加路由参数说明

参数	说明
目的地址类型	选择“IP 地址”。
目的地址	目的地址网段，设置为：0.0.0.0/0。
下一跳类型	在下拉列表中，选择类型“企业路由器”。
下一跳	选择下一跳资源。 下拉列表中将展示您创建的企业路由器名称。
描述	路由的描述信息，非必填项。 描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。

步骤四：开启 VPC 边界防火墙

1. 在左侧导航栏中，选择“资产管理 >VPC 边界防火墙管理”，进入“VPC 边界防火墙管理”页面。
2. 在“防火墙状态”侧，单击“开启防护”。
3. 单击“确认”，完成开启 VPC 边界防火墙。

后续操作

- 实现私网 IP 的细粒度防护：配置 NAT 防护规则，配置方式请参见 NAT 流量防护规则。
- 实现网络攻击拦截：配置入侵防御功能，请参见 3.5.2 配置入侵防御。
- 查看经过云防火墙的流量趋势和统计结果，请参见 3.6 流量分析，详细流量记录请参见流量日志。
- 开启防护后，流量默认放行，云防火墙将根据您设置的策略实施拦截：

表 3-37 设置策略

目标动作	操作指导
如果希望实现流量管控	可通过配置防护策略来进行处理，具体说明如下： • 通过防护规则放行/拦截流量： – 添加放行的防护规则：放行后的流量会经过入侵防御 IPS、病毒防御等功能的检测。 – 添加拦截的防护规则：流量将直接拦截。 • 通过黑白名单放行/拦截流量： – 添加白名单：流量将直接放行，不再经过其他功能的检测。 – 添加黑名单：流量将直接拦截。 详细操作请参见 3.4.2.1 通过防护规则拦截/放行流量或 3.4.2.5 通过黑白名单拦截/放行流量。
如果希望拦截网络攻击	可通过配置入侵防御来进行处理，详细操作请参见 3.5.2 配置入侵防御。

3.4 访问控制

3.4.1 访问控制策略概述

开启云防火墙防护时，系统默认放行所有流量。如果未配置访问控制策略，内部服务器与外网之间的通信将完全开放，无法有效管控未授权访问或内部威胁扩散。为此云

防火墙提供访问控制策略功能，可以通过自定义拦截或放行规则，对特定流量进行安全隔离，实现多方位防护。

访问控制策略类型

访问控制策略包括“防护规则”、“黑名单”、“白名单”功能，区别如表 3-38 所示，流量命中某一条策略时，执行该策略的动作，各功能的防护顺序请参见访问控制策略的防护顺序。

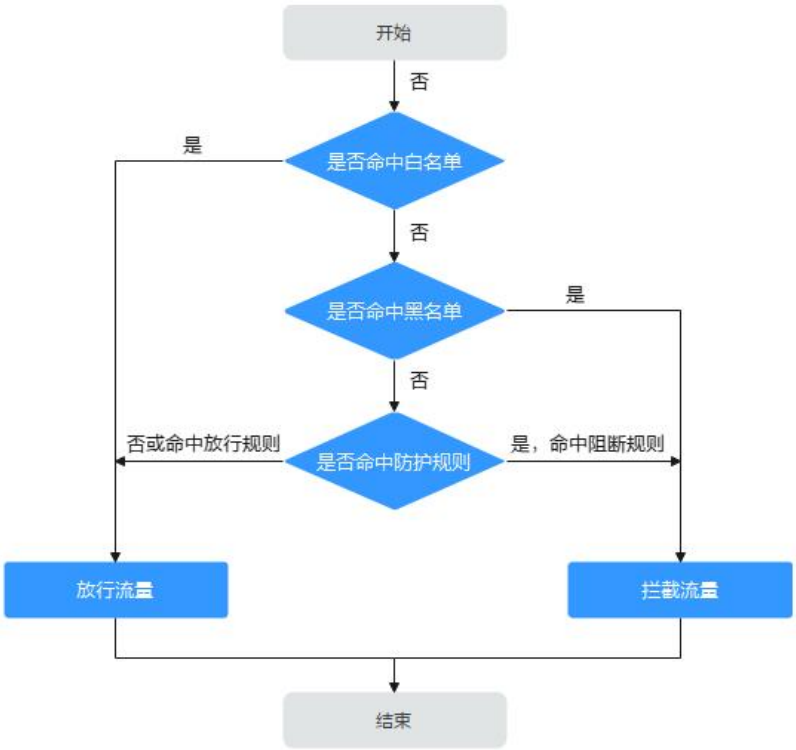
表 3-38 防护策略

-	防护规则	黑名单	白名单
支持的防护对象	• 五元组 • IP 地址组 • 地理位置（地域） • 域名和域名组（四层和七层流量） • 应用	• 五元组 • IP 地址组	• 五元组 • IP 地址组
网络类型	• 公网 IP • 私网 IP	• 公网 IP • 私网 IP	• 公网 IP • 私网 IP
防护后的动作	• 设置为“阻断”：流量直接拦截。 • 设置为“放行”：流量被“防护规则”功能放行后，再经过入侵防御（IPS）功能检测。	直接拦截流量。	流量被云防火墙放行，不再经过其它功能检测。
应用场景&特点	通过具体的特征识别指定流量，适用于需要精细化控制特定流量的情况；例如通过协议类型、端口号、应用等特征配置规则。	快速拦截已识别的安全威胁，适用于已知恶意流量数据的情况。	快速放行可信流量，适用于明确可信 IP 地址的情况。
配置方式	3.4.2.1 通过防护规则拦截/放行流量	3.4.2.5 通过黑白名单拦截/放行流量	3.4.2.5 通过黑白名单拦截/放行流量

访问控制策略的防护顺序

云防火墙匹配访问控制策略的防护优先级由高到低为：白名单 -> 黑名单 -> 防护策略（ACL）。

图 3-16 防护顺序



如需查看云防火墙的所有防护策略的防护顺序，请参见 4.1.8 云防火墙的防护顺序是什么？。

规格限制

VPC 边界防护和 NAT 流量防护，需满足专业版防火墙且开启 3.3.2 开启 VPC 边界流量防护防护。

配置阻断策略时注意事项

配置阻断 IP 的防护规则或黑名单时需注意以下几点：

1. 建议优先配置精准的 IP（如 192.168.10.5），减少网段配置，避免误拦截。
2. 对于反向代理 IP（如 Web 应用防火墙（WAF）的回源 IP），请谨慎配置阻断策略，建议配置放行的防护规则或白名单。
3. 对于正向代理 IP（如公司出口 IP），影响范围较大，请谨慎配置阻断策略。
4. 配置“地域”防护时，需考虑公网 IP 可能更换地址的情况。

防护规则中的防护元素

防护规则支持识别并匹配不同流量元素，实现对相关流量的放行或阻断。

匹配项	说明	配置类型	不同规则支持的配置类型
源	网络连接发起方	• IP：对特定的单个 IP 地址发起的流量进行访问控制。 • IP 地址组：对一系列 IP 地址发起的流量进行访问控制。 • 地域：对特定地理区域的 IP 地址发起的流量进行访问控制。 • Any：任意源地址。	• 互联网边界： – 外-内（入向策略）：IP 地址、IP 地址组、地域、ANY – 内-外（出向策略）：IP 地址、IP 地址组、ANY • NAT 网关： – 外-内（入向策略）：IP 地址、IP 地址组、地域、ANY – 内-外（出向策略）：IP 地址、IP 地址组、ANY • VPC 边界规则：IP 地址、IP 地址组、ANY

匹配项	说明	配置类型	不同规则支持的配置类型
目的	网络连接接收方	• IP：对特定的单个 IP 地址接收到的流量进行访问控制。 • IP 地址组：对一系列 IP 地址接收到的流量进行访问控制。 • 地域：对特定地理区域的 IP 地址接收到的流量进行访问控制。 • 域名/域名组：对域名地址接收到的流量进行访问控制。 如果防护规则的目的需要配置为域名或者域名组时，还需要了解如下两种域名识别模式： – 应用型：应用类型为 HTTP、HTTPS、TLS、SMTPS、POPS 时，云防火墙优先通过 Host 或 SNI 字段来实现域名的访问控制。 – 网络型：基于解析到的 IP 地址过滤；云防火墙对域名进行 DNS 解析，支持对解析出的 IP 地址进行访问控制。 • Any：任意目的地址。	• 互联网边界： – 外-内（入向策略）：IP 地址、IP 地址组、ANY – 内-外（出向策略）：IP 地址、IP 地址组、地域、域名/域名组、ANY • NAT 网关： – 外-内（入向策略）：IP 地址、IP 地址组、ANY – 内-外（出向策略）：IP 地址、IP 地址组、地域、域名/域名组、ANY • VPC 边界规则：IP 地址、IP 地址组、域名/域名组、ANY
服务	流量的协议类型或端口号	服务和服务组：表示指定一个服务或者多个服务的集合，通过指定协议类型、源端口、目的端口等信息来标识服务。 **服务**：设置协议类型、源端口和目的端口。 • 协议：传输层协议，支持选择 TCP、UDP、ICMP。 • 源端口：对访问流量发起的源端口进行访问控制。 • 目的端口：对访问流量的目的端口进行访问控制。 **服务组**：多个服务的集合。	ICMP 协议不支持配置端口。

匹配项	说明	配置类型	不同规则支持的配置类型
		ANY：不确定具体协议类型时可选择 ANY。	
应用	应用层协议	支持 HTTP、HTTPS、SMTP、SMTPS、SSL、POP3 等多种协议。 不确定具体应用类型时可选择 ANY。	取决于选择的协议类型。

配置示例：

参数名称	输入示例	说明
源/目的	0.0.0.0/0	所有 IP。
域名	www.example.com	对 www.example.com 域名生效。
	*.example.com	所有以 example.com 为后缀的域名，例如：test.example.com。
服务-源端口/目的端口	1-65535	所有端口生效。
	80-443	对 80 到 443 之间的所有端口生效。
	• 80 • 443	对 80 和 443 端口生效。

相关文档

- 添加单个防护规则实现流量防护，请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 添加单个黑/白名单实现流量防护请参见 3.4.2.5 通过黑白名单拦截/放行流量。
- 批量添加防护策略，请参见 3.4.4.1 导入/导出防护策略。
- 添加策略之后的后续操作：
  - 策略的命中情况，整体防护概况请参见 3.4.3 通过策略助手查看防护信息，详细日志请参见访问控制日志。
  - 流量趋势和统计结果，整体防护概况请参见 3.6 流量分析，详细流量记录请参见流量日志。
- 如果您的业务可能被防护策略误拦截，排查方式请参见 4.2.4 配置 CFW 防护策略后，业务无法访问怎么办？。

3.4.2 配置访问控制策略

3.4.2.1 通过防护规则拦截/放行流量

开启防护后，云防火墙默认放行所有流量，您可以配置防护规则，实现流量的拦截/放行。

防护规则说明

防护规则的防护对象、防护动作，以及防护场景说明如下：

名称	说明
支持的防护对象	• 五元组 • IP 地址组 • 地理位置（地域） • 域名和域名组（四层和七层流量） • 应用
网络类型	• 公网 IP • 私网 IP
防护后的动作	• 设置为“阻断”：流量直接拦截。 • 设置为“放行”：流量被“防护规则”功能放行后，再经过入侵防御（IPS）功能检测。
防护场景	防护规则支持防护以下几种场景： • 防护互联网边界中公网资产（EIP）的流量，请参见互联网边界防护规则。 • 防护互联网边界中私网资产的场景，请参见 NAT 流量防护规则。 • 防护 VPC 与 VPC 之间、VPC 与线下 IDC 之间的访问流量，请参见 VPC 边界防护规则。 **注意** 如果 IP 为 Web 应用防火墙（WAF）的回源 IP，建议配置放行的防护规则或白名单，请谨慎配置阻断的防护规则，否则可能会影响您的业务。 • 回源 IP 的相关信息请参见《Web 应用防火墙用户指南》中“放行 WAF 回源 IP”章节。 • 配置白名单请参见 3.4.2.5 通过黑白名单拦截/放行流量。

规格限制

仅“专业版”支持 VPC 边界防护和 NAT 流量（私网 IP）防护。

约束条件

- CFW 不支持应用层网关(Application Level Gateway，ALG)。如果有 ALG 相关业务(例如 SIP，FTP)，建议增加一条放通数据通道所有端口的规则（即“服务”为 Any，“防护动作”为放行）。
- CFW 长连接业务场景限制，配置策略的时候需要同时开启双向放通的安全策略，如果只开启单向策略，部分场景（开启和关闭防护）需要客户端重新发起连接。
- 配额限制：
  - 最多添加 20,000 条防护规则。
  - 单条防护规则最大限制如下：
    - 最多添加 20 个“IP 地址”（源和目的各 20 个）。
    - 最多关联 2 个“IP 地址组”（源和目的各 2 个）。
    - 最多关联 5 个服务组。
- 域名防护限制：
  - 域名防护时不支持添加中文域名格式。
  - 应用型域名引用数量限制如下：
    - 每个防火墙实例中最多引用 60,000 个域名。
    - 每个防火墙实例最多引用 1,000 个泛域名。
    - 每条防护规则最多引用 20,000 个域名。
    - 每条防护规则最多引用 128 个泛域名。

    计算方式：规则 A 和规则 B 中均引用了域名 1 和域名组 A（包含域名 2 和域名 3），则规则 A/B 引用的域名数量为 3 个，该防火墙实例中引用的域名数量为 6 个。
  - 网络型域名组最多解析 4,000 个 IP 地址，每个域名最多保存 1,000 个地址解析结果，超出时，可能导致无法正常访问对应的域名；对于解析结果较多或变化频繁的域名，如果防护流量是 HTTP、HTTPS 协议，建议优先使用应用型域名组添加策略。
  - 域名防护依赖于用户配置的域名服务器。默认域名服务器可能存在域名解析对应的 IP 地址不全，建议有访问自身业务相关域名场景时配置 3.8.2 DNS 服务器配置。
- 仅入方向规则（“方向”配置为“外-内”）的“源”地址支持配置“预定义地址组”。

对业务的影响

配置拦截的防护规则时，如果涉及地址转换或者存在代理的场景，需要谨慎评估拦截 IP 的影响。

互联网边界防护规则

步骤 1 开启弹性公网 IP 防护，请参见 3.3.1 开启互联网边界流量防护。

步骤 2 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入访问策略管理页面。

步骤 3 添加新的防护规则。

在“互联网边界”页签中，单击“添加”，在弹出的添加防护规则页面中，填写新的防护信息，填写规则请参见表 3-39。

表 3-39 添加防护规则-互联网边界

参数名称	参数说明
规则类型	选择“EIP 规则”：防护 EIP 的流量，仅支持配置公网 IP；配置私网 IP 请参见 NAT 流量防护规则。
IP 类型	支持选择 IPv4 或 IPv6。
名称	自定义安全策略规则的名称。
方向	“防护规则”选择 EIP 规则时，需要选择流量的方向： • 外-内：互联网访问云上资产（EIP）。 • 内-外：云上资产（EIP）访问互联网。
源	设置会话发起方。 • IP 地址：填写公网 IP 地址，支持设置单个 IP 地址、多个连续 IP 地址、地址段。 – 单个公网 IP 地址，如：xx.xx.10.5 – 多个连续的公网 IP 地址，中间使用“-”隔开，如：xx.xx.0.2-xx.xx.0.10 – 公网 IP 地址段，使用"/"隔开掩码，如：xx.xx.2.0/24 • IP 地址组：支持多个公网 IP 地址的集合。 “方向”配置为“外-内”时，“源”地址支持配置“预定义地址组”。 添加自定义 IP 地址组请参见添加自定义地址组，预定义地址组请参见查看预定义地址组。 • 地域：“方向”选择“外-内”时，支持地理位置防护，通过指定大洲、国家、地区配置防护规则。 • Any：任意源地址。

参数名称	参数说明
目的	设置会话接收方。 • IP 地址：填写公网 IP 地址，支持设置单个 IP 地址、多个连续 IP 地址、地址段。 – 单个公网 IP 地址，如：xx.xx.10.5 – 多个连续的公网 IP 地址，中间使用“-”隔开，如：xx.xx.0.2-xx.xx.0.10 – 公网 IP 地址段，使用"/"隔开掩码，如：xx.xx.2.0/24 • IP 地址组：支持多个公网 IP 地址的集合。 添加自定义 IP 地址组请参见添加自定义地址组。 • 地域：“方向”选择“内-外”时，支持地理位置防护，通过指定大洲、国家、地区配置防护规则。 • 域名/域名组：“方向”选择“内-外”时，支持域名或域名组的防护。 – 应用型：支持**域名**或**泛域名**的防护；适用应用层协议，支持 HTTP、HTTPS、TLS、SMTPS、POPS 的应用协议类型；通过域名匹配。 – 网络型：支持**单个域名**或**多个域名**的防护；适用网络层协议，支持所有协议类型；通过解析到的 IP 过滤。 说明 • 防护 HTTP、HTTPS、TLS、SMTPS、POPS 应用类型的**域名**时可选择任意类型。 • 防护 HTTP、HTTPS、TLS、SMTPS、POPS 应用类型的**泛域名（例如：*.example.com）**时仅支持选择“应用型”的任意选项。 • 防护其它应用类型（如 FTP、MySQL、SMTP）的**单个域名**：选择“网络型”的任意选项（选择“域名”时，解析出的 IP 地址上限个数为 600 个）。 • 防护其它应用类型（如 FTP、MySQL、SMTP）的**多个域名**：选择“网络型”“网络域名组”。 • 同一域名同时需要配置 HTTP/HTTPS/TLS/SMTPS/POPS（泛域名/应用型域名组）和其它应用类型（网络型域名组）时，“网络型”的防护规则“优先级”需高于“应用型”。 • 应用型与网络型详细介绍请参见添加域名组。 • Any：任意目的地址。

参数名称	参数说明
服务	• 服务：设置协议类型、源端口和目的端口。 – 协议：支持选择 TCP、UDP、ICMP。 – 源/目的端口：“协议”选择“TCP”或“UDP”时，需要设置端口号。 – 如您需设置该 IP 地址的全部端口，可配置“端口”为“1-65535”。 – 如您需设置某个端口，可填写为单个端口。例如设置 22 端口的访问，则配置“端口”为“22”。 – 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如设置 80-443 端口的访问，则配置“端口”为“80-443”。 • 服务组：支持多个服务（协议、源端口、目的端口）的集合。 添加自定义服务组请参见添加自定义服务组，预定义服务组请参见查看预定义服务组。 • Any：任意协议类型和端口号。
防护动作	设置流量经过防火墙时的处理动作。 • 放行：防火墙允许此流量转发。 • 阻断：防火墙禁止此流量转发。
启用状态	设置该策略是否立即启用。  ：表示立即启用，规则生效。  ：表示立即关闭，规则不生效。
策略优先级	设置该策略的优先级： • 置顶：表示将该策略的优先级设置为最高。 • 移动至选中规则后：表示将该策略优先级设置到某一规则后。 设置后，优先级数字越小，策略的优先级越高。 添加的第一条防护规则默认优先级是 1，无需选择“策略优先级”。
配置长连接	当前防护规则仅配置一个“服务”且“协议”选择“TCP”或“UDP”时，可配置业务会话老化时间（以秒为单位）。 最大支持 50 条规则设置长连接。 • 是：设置长连接时长。 • 否：保留默认时长，各协议规则默认支持的连接时长如下： – TCP 协议：1800s。 – UDP 协议：60s。

参数名称	参数说明
长连接时长	“配置长连接”选择“是”时，需要配置此参数。 设置长连接时长。输入“时”、“分”、“秒”。支持时长设置为 1 秒~1000 天。
标签	（可选）用于标识规则，可通过标签实现对安全策略的分类和搜索。
描述	（可选）标识该规则的使用场景和用途，以便后续运维时快速区分不同规则的作用。

步骤 4 单击“确认”，完成配置防护规则。

防护规则配置完成并处于启用状态时，会立即生效。

----结束

VPC 边界防护规则

步骤 1 开启 VPC 边界防火墙防护，请参见 3.3.2 开启 VPC 边界流量防护。

步骤 2 在左侧导航栏中，选择“访问控制 > 访问策略管理”，选择“VPC 边界”页签，进入 VPC 边界管理页面。

步骤 3 添加新的防护规则。

单击“添加”按钮，在弹出的“添加防护规则”中，填写新的防护信息，填写规则请参见表 3-40。

表 3-40 添加防护规则-VPC 边界

参数名称	参数说明
名称	自定义安全策略规则的名称。
方向	无需选择，VPC 间防护规则。
源	设置会话发起方。 • IP 地址：支持设置单个 IP 地址、多个连续 IP 地址、地址段。 – 单个 IP 地址，如：192.168.10.5 – 多个连续 IP 地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 • IP 地址组：支持多个 IP 地址的集合，添加 IP 地址组请参见添加 IP 地址组。 • Any：任意源地址。

参数名称	参数说明
目的	设置会话接收方。 • IP 地址：支持设置单个 IP 地址、多个连续 IP 地址、地址段。 – 单个 IP 地址，如：192.168.10.5 – 多个连续 IP 地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 • IP 地址组：支持多个 IP 地址的集合，添加 IP 地址组请参见添加 IP 地址组。 • Any：任意目的地址。
服务	设置访问流量的“协议”和“端口号”。 • 服务：设置协议类型、源端口和目的端口。 – 协议：支持选择 TCP、UDP、ICMP。 – 源/目的端口：“协议”选择“TCP”或“UDP”时，需要设置端口号。 – 如您需设置该 IP 地址的全部端口，可配置“端口”为“1-65535”。 – 如您需设置某个端口，可填写为单个端口。例如设置 22 端口的访问，则配置“端口”为“22”。 – 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如设置 80-443 端口的访问，则配置“端口”为“80-443”。 • 服务组：支持多个服务（协议、源端口、目的端口）的集合。 添加自定义服务组请参见添加服务组，预定义服务组请参见查看预定义服务组。 • Any：任意协议类型和端口号。
防护动作	设置流量经过防火墙时的处理动作。 • 放行：防火墙允许此流量转发。 • 阻断：防火墙禁止此流量转发。
启用状态	设置该策略是否立即启用。  ：表示立即启用，规则生效。  ：表示立即关闭，规则不生效。

参数名称	参数说明
策略优先级	设置该策略的优先级： • 置顶：表示将该策略的优先级设置为最高。 • 移动至选中规则后：表示将该策略优先级设置到某一规则后。 设置后，优先级数字越小，策略的优先级越高。 添加的第一条防护规则默认优先级是 1，无需选择“策略优先级”。
配置长连接	当前防护规则仅配置一个“服务”且“协议”选择“TCP”或“UDP”时，可配置业务会话老化时间（以秒为单位）。 最大支持 50 条规则设置长连接。 • 是：设置长连接时长。 • 否：保留默认时长，各协议规则默认支持的连接时长如下： – TCP 协议：1800s。 – UDP 协议：60s。
长连接时长	“配置长连接”选择“是”时，需要配置此参数。 设置长连接时长。输入“时”、“分”、“秒”。支持时长设置为 1 秒~1000 天。
标签	（可选）用于标识规则，可通过标签实现对安全策略的分类和搜索。
描述	（可选）标识该规则的使用场景和用途，以便后续运维时快速区分不同规则的作用。

步骤 4 单击“确认”，完成配置防护规则。

防护规则配置完成并处于启用状态时，会立即生效。

----结束

NAT 流量防护规则

步骤 1 开启 NAT 流量防护，请参见 3.3.3 开启 NAT 网关流量防护。

步骤 2 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入访问策略管理页面。

步骤 3 添加新的防护规则。

单击“添加”，在弹出的“添加防护规则”中，填写新的防护信息。

- DNAT 场景填写规则请参见表 3-41
- SNAT 场景填写规则请参见表 3-42。

表 3-41 添加防护规则-DNAT 场景

参数名称	参数说明

参数名称	参数说明
规则类型	选择 NAT 规则：防护 NAT 网关的流量，支持配置私网 IP。 **说明** NAT 规则需满足： • “专业版”防火墙。 • 已配置 VPC 边界防火墙。
名称	自定义安全策略规则的名称。
方向	选择“DNAT”。
源	设置会话发起方。 • IP 地址：填写公网 IP 地址，支持设置单个 IP 地址、多个连续 IP 地址、地址段。 – 单个公网 IP 地址，如：xx.xx.10.5 – 多个连续的公网 IP 地址，中间使用“-”隔开，如：xx.xx.0.2-xx.xx.0.10 – 公网 IP 地址段，使用"/"隔开掩码，如：xx.xx.2.0/24 • IP 地址组：支持多个公网 IP 地址的集合。 “方向”配置为“外-内”时，“源”地址支持配置“预定义地址组”。 添加自定义 IP 地址组请参见添加自定义地址组，预定义地址组请参见查看预定义地址组。 • 地域：支持地理位置防护，通过指定大洲、国家、地区配置防护规则。 • Any：任意源地址。
目的	设置会话接收方。 • IP 地址：填写私网 IP 地址，支持设置单个 IP 地址、多个连续 IP 地址、地址段。 – 单个 IP 地址，如：192.168.10.5 – 多个连续 IP 地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 • IP 地址组：支持多个私网 IP 地址的集合。 添加 IP 地址组请参见《云防火墙用户指南》中《添加 IP 地址组》。 • Any：任意目的地址。

参数名称	参数说明
服务	• 服务：设置协议类型、源端口和目的端口。 – 协议：支持选择 TCP、UDP、ICMP。 – 源/目的端口：“协议”选择“TCP”或“UDP”时，需要设置端口号。 – 如您需设置该 IP 地址的全部端口，可配置“端口”为“1-65535”。 – 如您需设置某个端口，可填写为单个端口。例如设置 22 端口的访问，则配置“端口”为“22”。 – 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如设置 80-443 端口的访问，则配置“端口”为“80-443”。 • 服务组：支持多个服务（协议、源端口、目的端口）的集合。 添加自定义服务组请参见添加自定义服务组，预定义服务组请参见查看预定义服务组。 • Any：任意协议类型和端口号。
防护动作	设置流量经过防火墙时的处理动作。 • 放行：防火墙允许此流量转发。 • 阻断：防火墙禁止此流量转发。
启用状态	设置该策略是否立即启用。  ：表示立即启用，规则生效。  ：表示立即关闭，规则不生效。
策略优先级	设置该策略的优先级： • 置顶：表示将该策略的优先级设置为最高。 • 移动至选中规则后：表示将该策略优先级设置到某一规则后。 设置后，优先级数字越小，策略的优先级越高。 添加的第一条防护规则默认优先级是 1，无需选择“策略优先级”。
配置长连接	当前防护规则仅配置一个“服务”且“协议”选择“TCP”或“UDP”时，可配置业务会话老化时间（以秒为单位）。 最大支持 50 条规则设置长连接。 • 是：设置长连接时长。 • 否：保留默认时长，各协议规则默认支持的连接时长如下： – TCP 协议：1800s。 – UDP 协议：60s。

参数名称	参数说明
长连接时长	“配置长连接”选择“是”时，需要配置此参数。 设置长连接时长。输入“时”、“分”、“秒”。支持时长设置为 1 秒~1000 天。
标签	（可选）用于标识规则，可通过标签实现对安全策略的分类和搜索。
描述	（可选）标识该规则的使用场景和用途，以便后续运维时快速区分不同规则的作用。

表 3-42 添加防护规则-SNAT 场景

参数名称	参数说明
规则类型	选择 NAT 规则：防护 NAT 网关的流量，支持配置私网 IP。 **说明** NAT 规则需满足： • “专业版”防火墙。 • 已配置 VPC 边界防火墙。
名称	自定义安全策略规则的名称。
方向	选择“SNAT”。
源	设置会话发起方。 • IP 地址：填写私网 IP 地址，支持设置单个 IP 地址、多个连续 IP 地址、地址段。 – 单个 IP 地址，如：192.168.10.5 – 多个连续 IP 地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 • IP 地址组：支持多个私网 IP 地址的集合。 添加 IP 地址组请参见添加自定义地址组。 • Any：任意源地址。

参数名称	参数说明
目的	设置会话接收方。 • IP 地址：填写公网 IP 地址，支持设置单个 IP 地址、多个连续 IP 地址、地址段。 – 单个公网 IP 地址，如：xx.xx.10.5 – 多个连续的公网 IP 地址，中间使用“-”隔开，如：xx.xx.0.2-xx.xx.0.10 – 公网 IP 地址段，使用"/"隔开掩码，如：xx.xx.2.0/24 • IP 地址组：支持多个公网 IP 地址的集合。 “方向”配置为“外-内”时，“源”地址支持配置“预定义地址组”。 添加自定义 IP 地址组请参见添加自定义地址组，预定义地址组请参见查看预定义地址组。 • 地域：支持地理位置防护，通过指定大洲、国家、地区配置防护规则。 • Any：任意目的地址。
服务	• 服务：设置协议类型、源端口和目的端口。 – 协议：支持选择 TCP、UDP、ICMP。 – 源/目的端口：“协议”选择“TCP”或“UDP”时，需要设置端口号。 – 如您需设置该 IP 地址的全部端口，可配置“端口”为“1-65535”。 – 如您需设置某个端口，可填写为单个端口。例如设置 22 端口的访问，则配置“端口”为“22”。 – 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如设置 80-443 端口的访问，则配置“端口”为“80-443”。 • 服务组：支持多个服务（协议、源端口、目的端口）的集合。 添加自定义服务组请参见添加自定义服务组，预定义服务组请参见查看预定义服务组。 • Any：任意协议类型和端口号。
防护动作	设置流量经过防火墙时的处理动作。 • 放行：防火墙允许此流量转发。 • 阻断：防火墙禁止此流量转发。
启用状态	设置该策略是否立即启用。  ：表示立即启用，规则生效。  ：表示立即关闭，规则不生效。

参数名称	参数说明
策略优先级	设置该策略的优先级： • 置顶：表示将该策略的优先级设置为最高。 • 移动至选中规则后：表示将该策略优先级设置到某一规则后。 设置后，优先级数字越小，策略的优先级越高。 添加的第一条防护规则默认优先级是 1，无需选择“策略优先级”。
配置长连接	当前防护规则仅配置一个“服务”且“协议”选择“TCP”或“UDP”时，可配置业务会话老化时间（以秒为单位）。 最大支持 50 条规则设置长连接。 • 是：设置长连接时长。 • 否：保留默认时长，各协议规则默认支持的连接时长如下： – TCP 协议：1800s。 – UDP 协议：60s。
长连接时长	“配置长连接”选择“是”时，需要配置此参数。 设置长连接时长。输入“时”、“分”、“秒”。支持时长设置为 1 秒~1000 天。
标签	（可选）用于标识规则，可通过标签实现对安全策略的分类和搜索。
描述	（可选）标识该规则的使用场景和用途，以便后续运维时快速区分不同规则的作用。

步骤 4 单击“确认”，完成配置防护规则。

防护规则配置完成并处于启用状态时，会立即生效。

----结束

查看防护规则的命中情况

您可以等待业务运行一段时间后，在防护规则列表的“命中次数”列查看防护规则的命中情况。

后续操作

查看防护效果：

- 策略的命中情况，整体防护概况请参见 3.4.3 通过策略助手查看防护信息，详细日志请参见访问控制日志。
- 流量趋势和统计结果，整体防护概况请参见 3.6 流量分析，详细流量记录请参见流量日志。

相关文档

- 批量添加防护规则请参见 3.4.4.1 导入/导出防护策略。
- 调整防护规则的优先级请参见 3.4.4.2 调整防护规则的优先级。

3.4.2.2 示例一：放行入方向中指定 IP 的访问流量

本文提供放行入方向中指定 IP 访问流量的配置示例，更多参数配置请参见 3.4.2.1 通过防护规则拦截/放行流量。

单独放行入方向中指定 IP 的访问流量

配置两条防护规则，一条拦截所有流量，优先级置于最低；一条单独放行指定 IP 的流量访问，优先级设置最高，其余参数可根据您的部署进行填写。

- 一条拦截所有流量，优先级置于最低，设置参数如下，其余参数可根据您的部署进行填写：

表 3-43 拦截所有流量

参数	示例	说明
方向	**外-内**	防护的流量的方向。
源	**Any**	网络流量的发起方。
目的	**Any**	网络流量的接收方。
服务	**Any**	网络流量的协议、源端口、目的端口。
应用	**Any**	针对应用层协议的防护策略。
动作	**阻断**	流量经过防火墙时的处理动作。

- 一条单独放行指定 IP 的流量访问，优先级设置最高，设置参数如下，其余参数可根据您的部署进行填写：

表 3-44 放行指定 IP

参数	示例	说明
方向	**外-内**	防护的流量的方向。
源	**IP 地址** **192.168.0.0**	网络流量的发起方。
目的	**Any**	网络流量的接收方。
服务	**Any**	网络流量的协议、源端口、目的端口。
应用	**Any**	针对应用层协议的防护策略。

参数	示例	说明
动作	**放行**	流量经过防火墙时的处理动作。

后续操作

查看防护效果：

- 策略的命中情况，整体防护概况请参见 3.4.3 通过策略助手查看防护信息，详细日志请参见访问控制日志。
- 流量趋势和统计结果，整体防护概况请参见 3.6 流量分析，详细流量记录请参见流量日志。

相关文档

- 防护规则的更多参数配置请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 黑白名单配置请参见 3.4.2.5 通过黑白名单拦截/放行流量。
- 批量添加防护策略，请参见 3.4.4.1 导入/导出防护策略。
- 拦截网络攻击请参见 3.5.2 配置入侵防御。
- 实现病毒防御请参见 3.5.3 配置病毒防御。

3.4.2.3 示例二：拦截某一地区的访问流量

本文提供拦截某一地区的访问流量的配置示例，更多参数配置请参见 3.4.2.1 通过防护规则拦截/放行流量。

拦截某一地区的访问流量

假如您需要拦截所有来源“北京”地区的访问流量，可以参照以下参数设置防护规则：

表 3-45 拦截某一地区的访问流量

参数	示例	说明
方向	**外-内**	防护的流量的方向。
源	**地域** **北京**	网络流量的发起方。
目的	**Any**	网络流量的接收方。
服务	**Any**	网络流量的协议、源端口、目的端口。
应用	**Any**	针对应用层协议的防护策略。
动作	**阻断**	流量经过防火墙时的处理动作。

后续操作

查看防护效果：

- 策略的命中情况，整体防护概况请参见 3.4.3 通过策略助手查看防护信息，详细日志请参见访问控制日志。
- 流量趋势和统计结果，整体防护概况请参见 3.6 流量分析，详细流量记录请参见流量日志。

相关文档

- 防护规则的更多参数配置请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 黑白名单配置请参见 3.4.2.5 通过黑白名单拦截/放行流量。
- 批量添加防护策略，请参见 3.4.4.1 导入/导出防护策略。
- 拦截网络攻击请参见 3.5.2 配置入侵防御。
- 实现病毒防御请参见 3.5.3 配置病毒防御。

3.4.2.4 示例三：配置 SNAT 的防护规则

本文提供 SNAT 防护的配置示例，更多参数配置请参见 3.4.2.1 通过防护规则拦截/放行流量。

SNAT 防护配置

假如您的私网 IP 为“10.1.1.2”，通过 NAT 网关访问的外部域名为“www.example.com”，您可以参照以下参数配置 NAT 防护，其余参数可根据您的部署进行填写：

表 3-46 添加 NAT 防护规则

参数	示例	说明
方向	**SNAT**	防护的流量的方向。
源	**IP 地址** **10.1.1.2**	网络流量的发起方。
目的	**域名/域名组** **网络型** **www.example.com**	网络流量的接收方。
服务	**服务** **TCP、1-65535、1-65535**	网络流量的协议、源端口、目的端口。
应用	**应用** **HTTP、HTTPS**	针对应用层协议的防护策略。
防护动作	**放行**	流量经过防火墙时的处理动作。

后续操作

查看防护效果：

- 策略的命中情况，整体防护概况请参见 3.4.3 通过策略助手查看防护信息，详细日志请参见访问控制日志。
- 流量趋势和统计结果，整体防护概况请参见 3.6 流量分析，详细流量记录请参见流量日志。

相关文档

- 防护规则的更多参数配置请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 黑白名单配置请参见 3.4.2.5 通过黑白名单拦截/放行流量。
- 批量添加防护策略，请参见 3.4.4.1 导入/导出防护策略。
- 拦截网络攻击请参见 3.5.2 配置入侵防御。
- 实现病毒防御请参见 3.5.3 配置病毒防御。

3.4.2.5 通过黑白名单拦截/放行流量

开启防护后，云防火墙默认放行所有流量，您可以通过配置黑/白名单规则，拦截/放行 IP 地址的访问请求。

本文指导您添加单个黑白名单，如果需要批量添加黑白名单请参见 3.4.4.1 导入/导出防护策略。

黑白名单策略说明

黑白名单策略的防护对象、防护动作，以及应用场景说明如下：

名称	说明
支持的防护对象	• 五元组 • IP 地址组
网络类型	• 公网 IP • 私网 IP
防护后的动作	• 黑名单：直接拦截流量。 • 白名单：流量被云防火墙放行，不再经过其它功能检测。
应用场景	• 黑名单：适用于已知恶意流量数据的情况。 • 白名单：适用于明确可信 IP 地址的情况。 **注意** 如果 IP 为 Web 应用防火墙（WAF）的回源 IP，建议使用白名单或配置放行的防护规则，请谨慎配置黑名单规则，否则可能会影响您的业务。 • 回源 IP 的相关信息请参见《Web 应用防火墙用户指南》中《放行 WAF 回源 IP》。 • 配置防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。

规格限制

- 云防火墙最多支持配置 2000 条黑名单和 2000 条白名单。

  当您需要配置的黑名单 IP 或白名单 IP 超出限制时，可通过添加 IP 地址组，并在防护规则中引用的方式实现拦截/放行效果。

  - 添加 IP 地址组请参见添加自定义地址组。
  - 添加防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 私网 IP 防护，需满足专业版防火墙且开启 3.3.2 开启 VPC 边界流量防护防护。

系统影响

- 将 IP 或 IP 地址段配置为黑名单/白名单后，来自该 IP 或 IP 地址段的访问，CFW 将不会做任何检测，直接拦截（黑名单）/放行（白名单），您可以在 3.7.2 日志查询中检索该 IP 或 IP 地址段查看访问情况和流量情况。
- 配置黑名单时，如果涉及地址转换或者存在代理的场景，需要谨慎评估拦截 IP 的影响。

通过添加黑白名单拦截/放行流量

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”界面。切换防护对象页签后，选择“黑名单”或“白名单”页签。

步骤 5 单击“添加”，设置地址方向、IP 地址、协议类型、端口，填写规则请参见表 3-47。

表 3-47 黑/白名单

参数名称	参数说明
地址方向	选择“源地址”或“目的地址”。 • 源地址：设置会话发起方。 • 目的地址：设置会话接收方。
协议类型	协议类型当前支持：TCP、UDP、ICMP、Any。

参数名称	参数说明
端口	“协议类型”选择“TCP”或“UDP”时，设置需要放行或拦截的端口。 • 如您需设置该 IP 地址的全部端口，可配置“端口”为“1-65535”。 • 如您需设置某个端口，可填写为单个端口。例如放行/拦截该 IP 地址 22 端口的访问，则配置“端口”为“22”。 • 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如放行/拦截该 IP 地址 80-443 端口的访问，则配置“端口”为“80-443”。
IP 地址列表	• 自定义 IP 地址：在输入框中输入单个或多个 IP 地址，单击“解析”，将 IP 地址加入列表中。 • 预定义地址组：单击“添加预定义地址组”，在弹出的对话框中选择地址组，预定义地址组介绍请参见查看预定义地址组。 **注意** “WAF 回源 IP 地址组”添加至黑/白名单后，如果回源 IP 改变，您需手动修改对应黑/白名单中的 IP 地址。
描述	（可选）设置该黑/白名单的备注信息。

步骤 6 单击“确认”，完成添加。

----结束

相关文档

- 编辑和删除黑白名单请参见 3.4.4.4 管理黑白名单。
- 批量添加黑白名单请参见 3.4.4.1 导入/导出防护策略。
- 添加更精细化的访问控制您可以配置防护规则，请参见 3.4.2 配置访问控制策略。
- 拦截恶意攻击请参见 3.5 攻击防御。

3.4.3 通过策略助手查看防护信息

配置防护策略后，您可通过策略助手快速查看 7 天内防护规则的命中情况，及时调整防护规则。

通过策略助手查看防护信息

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 策略助手”，进入策略助手页面。

步骤 5 查看防火墙实例下防护规则的统计信息。

- 策略看板：查看指定时间段内防护策略（防护规则和黑白名单）命中/放行/阻断的总数，以及高频命中的放行/阻断策略。
- 策略命中情况：查看指定时间段内指定规则的命中详情。
- 可视化统计：查看指定时间段内访问规则拦截的攻击事件中指定参数的 TOP 5 排行，参数说明请参见表 3-48。单击单条数据查看策略命中详情，参数说明请参见表 3-70。

表 3-48 策略助手可视化统计参数说明

参数名称	参数说明
TOP 命中拦截策略	命中且执行拦截的策略。
TOP 出云拦截 IP	出方向流量中被拦截的 IP，切换“源”或“目的”查看源 IP 或目的 IP。
TOP 入云拦截 IP	入方向流量中被拦截的 IP，切换“源”或“目的”查看源 IP 或目的 IP。
TOP 拦截目的端口	拦截的目的端口，切换“出云”或“入云”查看出方向或入方向。
TOP 拦截 IP 地区	拦截的 IP 所属地区，切换“出云的目的”或“入云的源”查看出方向目的 IP 或入方向的源 IP。

- 长期未命中策略：查看一周、一个月、三个月或六个月内启用后无命中的策略，建议您及时修改或删除。

----结束

相关文档

- 添加单个防护规则实现流量防护，请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 添加单个黑/白名单实现流量防护请参见 3.4.2.5 通过黑白名单拦截/放行流量。
- 批量添加防护策略，请参见 3.4.4.1 导入/导出防护策略。
- 如果您的业务可能被防护策略误拦截，排查方式请参见 4.2.4 配置 CFW 防护策略后，业务无法访问怎么办？。

3.4.4 管理访问控制策略

3.4.4.1 导入/导出防护策略

如果您需批量添加和导出防护规则、黑/白名单、IP 地址组、服务组、域名组，请参照本章节进行处理。

规格限制

如果业务需要导入/导出 VPC 边界防护策略，请确认防火墙版本是“专业版”。

批量导入防护策略

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤 5 单击页面右上方“下载中心”，右侧弹出“下载中心”页面。

步骤 6 单击“下载模板”，下载导入规则模板到本地。

步骤 7 请按表格要求填写您要添加的防护策略信息。

- 导入限制：
  - 最大支持每个页签中单次导入 640 条规则/成员。
  - 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。
- 参数说明：
  - 防护规则参数说明：
    - 互联网边界防护规则参数说明请参见导入规则模板参数-防护规则表（互联网边界防护规则）
    - VPC 边界防护规则参数说明请参见导入规则模板参数-VPC 防护规则表（VPC 边界防护规则）。
  - 黑白名单参数说明请参见 3.4.2.5 通过黑白名单拦截/放行流量。
  - IP 地址组参数说明请参见 3.4.5.1 管理 IP 地址组。
  - 服务组参数说明请参见 3.4.5.3 管理服务组。
  - 域名组参数说明请参见 3.4.5.2 管理域名组。

步骤 8 表格填写完成后，单击“导入规则”，导入防护规则表。

说明

- 导入规则操作将在数分钟内完成。
- 导入规则过程中访问策略、IP 地址组、服务组均不支持添加、编辑和删除操作。
- 导入后的策略优先级低于已创建的策略。

步骤 9 单击“下载中心”，查看导入规则任务状态，任务状态显示“导入成功”表示导入防护规则成功。

步骤 10 返回防护规则列表查看导入的防护规则。

----结束

批量导出防护策略

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤 5 单击页面右上方“下载中心”，右侧弹出“下载中心”页面。

步骤 6 单击“导出规则”，导出规则到本地。

----结束

导入规则模板参数-防护规则表（互联网边界防护规则）

表 3-49 互联网边界防护规则表参数说明

参数名称	参数说明	取值样例
顺序	定义规则序号。	1
规则名称	自定义规则名称。 只能由中文、字母、数字、下划线、连接符或空格任意一种或多种字符类型组成，且名称长度不能超过 255 个字符。	test
防护规则	选择安全策略的防护类型。 • EIP 防护：防护 EIP 的流量，仅支持配置公网 IP。 • NAT 防护：防护 NAT 的流量，可以配置私网 IP。	EIP 防护
方向	选择防护方向： • 外-内：外网访问内部服务器。 • 内-外：客户服务器访问外网。	内到外
动作	选择“放行”或者“阻断”。设置防火墙对通过流量的处理动作。	放行
规则地址类型	选择“IPv4”或者“IPv6”。设置防护的 IP 类型。	IPv4
启用状态	选择该策略是否立即启用。 • 启用：表示立即开启，规则生效； • 禁用：表示关闭，规则不生效。	启用
描述	自定义规则描述。	test

参数名称	参数说明	取值样例
源地址类型	选择会话发起方的类型。 • **IP 地址**：支持设置单个 IP 地址、连续多个 IP 地址、地址段。 • **IP 地址组**：支持多个 IP 地址的集合。 • **地域**：支持按照地域防护。	IP 地址
源 IP 地址	“源地址类型”选择“IP 地址”时，需填写“源 IP 地址”。 支持以下输入格式： • 单个 IP 地址，如：192.168.10.5 • 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 • 地址段，使用“/”隔开掩码，如：192.168.2.0/24 如果您希望输入多个单 IP 地址或多个 IP 地址段，需要配置多条规则。这些规则的 IP 地址（段）不同，其他参数相同。	192.168.10.5
源地址组名称	“源地址类型”选择“IP 地址组”时，需填写“源地址组名称”。 支持以下输入格式； • 可输入中文、字母、数字、下划线、连接符或空格。 • 名称长度不能超过 255 个字符。	s_test
源大洲地域	“源地址类型”选择“地域”时，需填写“源大洲地域”。 您可以切换模板表格至“大洲信息表”页签，查看大洲信息。	AS:亚洲
源国家地域	“源地址类型”选择“地域”时，需填写“源国家地域”。 您可以切换模板表格至“国家信息表”页签，查看国家信息。	CN:中国大陆

参数名称	参数说明	取值样例
目的地址类型	选择会话接收方的类型。 • **IP 地址**：支持设置单个 IP 地址、连续多个 IP 地址、地址段。 • **IP 地址组**：支持多个 IP 地址的集合。 • **域名**：由一串用点分隔的英文字母组成（以字符串的形式来表示服务器 IP），用户通过域名来访问网站。 • **域名组**：支持多个域名的集合。 • **地域**：支持地域防护。	IP 地址组
目的 IP 地址	“目的地址类型”选择“IP 地址”时，需填写“目的 IP 地址”。 目的 IP 地址支持以下输入格式： • 单个 IP 地址，如：192.168.10.5 • 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 • 地址段，使用“/”隔开掩码，如：192.168.2.0/24 如果您希望输入多个单 IP 地址或多个 IP 地址段，需要配置多条规则。这些规则的 IP 地址（段）不同，其他参数相同。	192.168.10.6
目的地址组名称	“目的地址类型”选择“IP 地址组”时，需填写“目的地址组名称”。 支持以下输入格式； • 可输入中文、字母、数字、下划线、连接符或空格。 • 名称长度不能超过 255 个字符。	d_test
目的大洲地域	“目的地址类型”选择“地域”时，需填写“目的大洲地域”。 您可以切换模板表格至“大洲信息表”页签，查看大洲信息。	AS:亚洲
目的国家地域	“目的地址类型”选择“地域”时，需填写“目的国家地域”。 您可以切换模板表格至“国家信息表”页签，查看国家信息。	CN:中国大陆
域名	“目的地址类型”选择“域名”时，需填写“域名”。 由一串用点分隔的英文字母组成（以字符串的形式来表示服务器 IP），用户通过域名来访问网站。	www.example.com

参数名称	参数说明	取值样例
目的域名组名称	“目的地址类型”选择“域名组”时，需填写“目的域名组名称”。 输入域名组名称。	域名组 1
服务类型	选择**服务**或**服务组**。 • **服务**：支持设置单个服务。 • **服务组**：支持多个服务的集合。	服务
协议/源端口/目的端口	设置需要限制的类型。 • 协议类型当前支持：TCP、UDP、ICMP、Any。 • 设置需要开放或限制的源端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443 • 设置需要开放或限制的目的端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443	TCP/443/443
服务组名称	自定义服务组名称。 只能由中文、字母、数字、下划线、连接符或空格任意一种或多种字符类型组成，且名称长度不能超过 255 个字符。	service_test
分组标签	用于标识规则，可通过标签实现对安全策略的分类和搜索。	k=a

导入规则模板参数-VPC 防护规则表（VPC 边界防护规则）

表 3-50 VPC 边界防护规则表参数说明

参数名称	参数说明	取值样例
顺序	定义规则序号。	1
规则名称	自定义规则名称。 只能由中文、字母、数字、下划线、连接符或空格任意一种或多种字符类型组成，且名称长度不能超过 255 个字符。	test
动作	选择“放行”或者“阻断”。设置防火墙对通过流量的处理动作。	放行

参数名称	参数说明	取值样例
启用状态	选择该策略是否立即启用。 • 启用：表示启用，规则生效； • 禁用：表示关闭，规则不生效。	启用
描述	自定义规则描述。	test
源地址类型	设置会话发起方的类型。 • **IP 地址**：支持设置单个 IP 地址、连续多个 IP 地址、地址段。 • **IP 地址组**：支持多个 IP 地址的集合。	IP 地址
源 IP 地址	“源地址类型”选择“IP 地址”时，需填写“源 IP 地址”。 支持以下输入格式： • 单个 IP 地址，如：192.168.10.5 • 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 • 地址段，使用“/”隔开掩码，如：192.168.2.0/24 如果您希望输入多个单 IP 地址或多个 IP 地址段，需要配置多条规则。这些规则的 IP 地址（段）不同，其他参数相同。	192.168.10.5
源地址组名称	“源地址类型”选择“IP 地址组”时，需填写“源地址组名称”。 支持以下输入格式； • 可输入中文、字母、数字、下划线、连接符或空格。 • 名称长度不能超过 255 个字符。	s_test
目的地址类型	选择会话接收方的类型。 • **IP 地址**：支持设置单个 IP 地址、连续多个 IP 地址、地址段。 • **IP 地址组**：支持多个 IP 地址的集合。	IP 地址组

参数名称	参数说明	取值样例
目的 IP 地址	“目的地址类型”选择“IP 地址”时，需填写“目的 IP 地址”。 目的 IP 地址支持以下输入格式： • 单个 IP 地址，如：192.168.10.5 • 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 • 地址段，使用“/”隔开掩码，如：192.168.2.0/24 如果您希望输入多个单 IP 地址或多个 IP 地址段，需要配置多条规则。这些规则的 IP 地址（段）不同，其他参数相同。	192.168.10.6
目的地址组名称	“目的地址类型”选择“IP 地址组”时，需填写“目的地址组名称”。 支持以下输入格式； • 可输入中文、字母、数字、下划线、连接符或空格。 • 名称长度不能超过 255 个字符。	d_test
服务类型	选择**服务**或**服务组**。 • **服务**：支持设置单个服务。 • **服务组**：支持多个服务的集合。	服务
协议/源端口/目的端口	设置需要限制的类型。 • 协议类型当前支持：TCP、UDP、ICMP、Any。 • 设置需要开放或限制的源端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443 • 设置需要开放或限制的目的端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443	TCP/443/443
服务组名称	自定义服务组名称。 只能由中文、字母、数字、下划线、连接符或空格任意一种或多种字符类型组成，且名称长度不能超过 255 个字符。	service_test
分组标签	用于标识规则，可通过标签实现对安全策略的分类和搜索。	k=a

相关文档

- 添加单个防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 添加黑/白名单请参见 3.4.2.5 通过黑白名单拦截/放行流量。
- 查看防护效果：
  - 策略的命中情况，整体防护概况请参见 3.4.3 通过策略助手查看防护信息，详细日志请参见访问控制日志。
  - 流量趋势和统计结果，整体防护概况请参见 3.6 流量分析，详细流量记录请参见流量日志。
- 调整防护规则的匹配优先级请参见 3.4.4.2 调整防护规则的优先级。

3.4.4.2 调整防护规则的优先级

流量命中某一条规则时，执行该规则的动作，并结束防护规则的匹配。建议设置放行的规则优先级高于阻断的规则，具体化的规则优先级高于宽泛的规则。

本文指导您调整防护规则的优先级顺序。

优先级排序

数字越大，优先级越低，1 是最高优先级。

调整防护规则的优先级

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤 5 在需要调整优先级的防护规则所在行的“操作”列，单击“设置优先级”。

步骤 6 选择“置顶”，或“移动至选中规则后”。

- 选择置顶，表示将该策略设置为最高优先级。
- 选择“移动至选中规则后”，需要选择相应的规则，表示将该策略优先级设置到选择的规则之后。

步骤 7 单击“确认”，完成设置优先级。

----结束

相关文档

- 添加单个防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 添加黑/白名单请参见 3.4.2.5 通过黑白名单拦截/放行流量。
- 查看防护效果：

- 策略的命中情况，整体防护概况请参见 3.4.3 通过策略助手查看防护信息，详细日志请参见访问控制日志。
- 流量趋势和统计结果，整体防护概况请参见 3.6 流量分析，详细流量记录请参见流量日志。

- 批量添加防护策略请参见 3.4.4.1 导入/导出防护策略。

3.4.4.3 管理防护规则

本节介绍防护规则页面的参数信息和防护规则的编辑、复制、删除操作。

其中复制操作生成的新防护规则“优先级”默认为“1”（优先级最高）。

查看防护规则

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面，根据需要选择“互联网边界”或“VPC 边界”页签，进入目标防护规则管理页面。

表 3-51 查看防护规则

参数名称	参数说明
优先级	当前规则的优先级别。 数字越小策略的优先级越高。
名称/规则 ID	自定义规则名称和 ID。
启用状态	当前规则的启用状态，支持启用和禁用。
方向	防护规则的流量方向。
源	访问流量中的会话发起方。
目的	访问流量中的会话接收方。
服务	• 协议类型当前支持：TCP、UDP、ICMP、Any。 • 源端口：当前开放或限制的源端口号。支持单个端口，或者连续端口组，中间使用“-”隔开，如：80-443。 • 目的端口：当前开放或限制的目的端口号。 支持单个端口，或者连续端口组，中间使用“-”隔开，如：80-443。
应用	访问流量中的应用类型。

参数名称	参数说明
动作	• “放行”：设置相应流量通过防火墙。 • “阻断”：阻止相应流量通过防火墙。
命中次数	当前规则已放行或阻断的累计命中次数（距上一次清零前），命中详情请参见访问控制日志。
时间计划	设置的规则生效时间。
标签	当前规则设置的标签信息。

步骤 5 （可选）根据您的需要在方向或协议类型下拉框选择需要查看的方向或协议类型。

----结束

编辑防护规则

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面，根据需要选择“互联网边界”或“VPC 边界”页签。

步骤 5 在需要编辑的防护规则所在行的“操作”列，单击“编辑”。

步骤 6 在系统弹出编辑防护规则中，修改您需修改的参数信息。

步骤 7 修改完成后，单击“确认”保存。

----结束

复制防护规则

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面，根据需要选择“互联网边界”或“VPC 边界”页签。

步骤 5 在需要复制的防护规则所在行的“操作”列，单击“更多 > 复制”。

步骤 6 修改参数后，单击“确认”，新生成的防护规则“优先级”默认为“1”（优先级最高）。

----结束

删除防护规则

警告

删除规则后无法恢复，请谨慎操作。

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面，根据需要选择“互联网边界”或“VPC 边界”页签。

步骤 5 在需要删除的防护规则所在行的“操作”列，单击“更多 > 删除”。

步骤 6 在弹出的“删除规则”界面，输入“DELETE”，单击“确定”，完成删除。

----结束

相关文档

- 添加单个防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 添加黑/白名单请参见 3.4.2.5 通过黑白名单拦截/放行流量。
- 查看防护效果：
  - 策略的命中情况，整体防护概况请参见 3.4.3 通过策略助手查看防护信息，详细日志请参见访问控制日志。
  - 流量趋势和统计结果，整体防护概况请参见 3.6 流量分析，详细流量记录请参见流量日志。
- 批量添加防护策略请参见 3.4.4.1 导入/导出防护策略。
- 调整防护规则的匹配优先级请参见 3.4.4.2 调整防护规则的优先级。

3.4.4.4 管理黑白名单

本节介绍黑白名单的编辑、删除操作。

编辑黑/白名单

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面，根据需要选择“互联网边界”或“VPC 边界”页签。

步骤 5 选择“黑名单”或“白名单”页签。

步骤 6 在需要编辑的规则所在行的“操作”列中，单击“编辑”。

对参数进行修改，参数详情请参见 3.4.2.5 通过黑白名单拦截/放行流量。

步骤 7 修改完成后，单击“确认”保存。

----结束

删除黑/白名单

警告

删除名单后无法恢复，请谨慎操作。

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面，根据需要选择“互联网边界”或“VPC 边界”页签。

步骤 5 选择“黑名单”或“白名单”页签。

步骤 6 在需要删除的规则所在行的“操作”列，单击“删除”。

步骤 7 在弹出的“删除黑名单”或“删除白名单”界面，确认删除的信息无误后，输入“DELETE”，单击“确定”，完成删除。

----结束

3.4.5 管理对象组

3.4.5.1 管理 IP 地址组

操作场景

IP 地址组是多个 IP 地址的集合。通过在访问规则中一键引用 IP 地址组，即可实现对特定对象群体的统一流量管控。此外，当 IP 地址组更新时会自动同步至所有关联策略，无需手动调整。这不仅能提升策略调整响应速度，还可以降低重复配置工作量，实现运维效率的全面提升。

约束与限制

- 添加自定义 IP 地址组和 IP 地址：
  - 每个防火墙实例下最多添加 3,800 个 IP 地址组。
  - 每个 IP 地址组中最多添加 640 个 IP 地址成员，且单次最多可添加 100 个 IP 地址成员。
  - 每个防火墙实例下最多添加 30,000 个 IP 地址。
- 预定义地址组仅支持查看，不支持添加、修改、删除操作。
- 被防护规则引用的地址组不支持删除，需优先调整/删除对应规则。

添加自定义地址组

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3（可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤 5 在“IP 地址组”页签的自定义地址组页面中，单击“添加 IP 地址组”，弹出添加 IP 地址组界面，填写 IP 地址组信息。

表 3-52 添加 IP 地址组的参数说明

参数	说明
地址组类型	选择地址组类型，支持“IPv4”和“IPv6”。 **说明** 仅专业版支持选择 IPv6，标准版默认防护 IPv4。
IP 地址组名称	需要添加的 IP 地址组名称。 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。
IP 地址列表	添加需要管理的 IP 地址，单击“解析”至 IP 地址列表中。 输入规则如下： • 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 IP 地址，使用半角逗号（,）、半角分号（;）、换行符、制表符或空格隔开，如 192.168.1.0,192.168.1.0/24。

参数	说明
描述	标识该 IP 组的使用场景和用途，以便后续运维时快速区分不同的 IP 组。 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）、空格和特殊字符（-_）。 • 长度不超过 255 字符。

步骤 6 确认无误后，单击“确定”，完成添加 IP 地址组。

----结束

添加自定义地址组中 IP 地址

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤 5 在“IP 地址组”页签的自定义地址组页面中，单击目标 IP 地址组名称，弹出“IP 地址组详情”界面。

步骤 6 单击“添加 IP 地址”，弹出“添加 IP 地址”界面，添加 IP 地址。

- 批量添加 IP 地址：在输入框中添加需要管理的 IP 地址，单击“解析”至 IP 地址列表中。

  输入规则如下：

  - 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 IP 地址，使用半角逗号（,）、半角分号（;）、换行符、制表符或空格隔开，如 192.168.1.0,192.168.1.0/24。
- 添加单个 IP 地址：在 IP 地址列表上方单击“添加”，输入“IP 地址”和“描述”信息。

步骤 7 确认信息无误后，单击“确认”，完成添加 IP 地址。

----结束

查看预定义地址组

云防火墙为您提供 NAT64 转换地址组，建议您配置放行的策略。

- NAT64 转换地址组：提供转换后的 IP 地址；开启弹性公网 IP（EIP）服务的 IPv6 转换功能后，云防火墙接收到对应 IPv6 流量的源 IP 地址会被转换为当前地址组中的 IP。

说明

如果您开启了弹性公网 IP（EIP）服务的 IPv6 转换功能，建议放行 NAT64 转换地址组。

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤 5 在“IP 地址组”页签中，选择“预定义地址组”页签，单击目标地址组的名称，进入详细信息页面。

步骤 6 查看预定义地址组的名称、类型、已添加的 IP 地址等信息。

----结束

删除自定义 IP 地址组

警告

删除 IP 地址组后无法恢复，请谨慎操作。

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤 5 删除自定义 IP 地址组。

- 删除单个自定义 IP 地址组
  a. 在 IP 地址组页签的自定义地址组页面中，单击目标 IP 地址组所在行“操作”列的“删除”。
  b. 在弹出的确认框中，确认信息无误后，输入“DELETE”，单击“确定”。
- 批量删除自定义 IP 地址组
  a. 在 IP 地址组页签的自定义地址组页面的 IP 地址组表格中，批量勾选 IP 地址组后，单击列表上方的“删除”。
  b. 在弹出的确认框中，确认信息无误后，输入“DELETE”，单击“确定”。

----结束

相关操作

- 导出 IP 地址组：单击列表上方的“导出”，选择需要的数据范围。
- 批量删除 IP 地址：在“IP 地址组详情”界面，批量勾选 IP 地址后，单击列表上方的“删除”，确认无误后单击“确定”。

3.4.5.2 管理域名组

操作场景

域名组是多个域名或泛域名（泛域名标准格式为*.域名，其中*是通配符，表示匹配任意字符或字符串，例如：*.example.com）的集合。通过在访问规则中一键引用域名组，即可实现对特定对象群体的统一流量管控。此外，当域名组更新时会自动同步至所有关联策略，无需手动调整。这不仅能提升策略调整响应速度，还可以降低重复配置工作量，实现运维效率的全面提升。

域名组类型

CFW 提供应用域名组（七层协议解析）和网络域名组（四层协议解析）两种类型，两类域名组的差异如表 3-53 所示。

表 3-53 域名组类型

-	应用域名组（七层协议解析）	网络域名组（四层协议解析）
防护对象	• 域名 • 泛域名	• 单个域名 • 多个域名
协议类型	应用层协议，支持 HTTP、HTTPS、TLS、SMTPS、POPS 的应用协议类型。	网络层协议，支持所有协议类型。
匹配规则	基于域名匹配；将会话中的 HOST 字段与应用型域名进行比对，如果一致，则命中对应的防护规则。	基于解析到的 IP 地址过滤。 在后台获取 DNS 服务器解析出的 IP 地址（每 15s 获取一次），当会话的四元组与网络型域名相关规则匹配、且本次访问解析到的地址在此前保存的结果中（已从 DNS 服务器解析中获取到 IP 地址），则命中对应的防护规则。
配置建议	映射地址量大或映射结果变化快的域名建议优先使用应用域名组（如被内容分发网络（CDN）加速的域名）。	

约束与限制

- 添加域名组：
  - 域名组成员不支持添加中文域名格式。

- 两类域名组的约束与限制如下：
  - 应用域名组（七层协议解析）
    - 每个防火墙实例下最多添加 500 个域名组。
    - 每个防火墙实例下最多添加 2500 个域名成员。
    - 每个应用域名组中最多添加 1500 个域名成员，且单次最多可添加 500 个域名成员。
  - 网络域名组（四层协议解析）
    - 每个防火墙实例下最多添加 1000 个域名成员。
    - 每个网络域名组中最多添加 15 个域名成员。
    - 每个域名组最多支持解析 1500 条 IP 地址。
    - 每个域名最多支持解析 1000 条 IP 地址。
- 被防护规则引用的域名组不支持删除，需优先调整/删除对应规则。

添加域名组

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤 5 切换至“域名组”页签。

（可选）如果添加网络域名组，则请在进入域名组页面后选择“网络域名组”页签。

步骤 6 在应用域名组或网络域名组页面中，单击“添加域名组”，并在弹出“添加域名组”页面中填写域名组信息。

表 3-54 添加域名组参数说明

参数名称	参数说明
域名组类型	应用型/网络型
域名组名称	自定义域名组名称。
域名	输入域名，单击“解析”至域名列表中，输入规则如下： • 支持多级别单域名（例如，一级域名 example.com，二级域名 www.example.com 等）和泛域名（例如：*.example.com）。 • 多个域名以英文逗号、英文分号、换行符、空格分隔。 • 输入的域名请勿重复。
描述	（可选）设置该域名组的备注信息。

步骤 7 确认填写信息无误后，单击“确认”，完成添加域名组。

----结束

添加域名组中域名

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤 5 切换至“域名组”页签，进入域名组页面后，单击目标域名组名称，弹出域名组详情页面。

如果添加网络域名组域名，则请在进入域名组页面后，选择“网络域名组”页签，单击目标域名组名称，弹出“域名组详情”弹窗。

步骤 6 单击“添加域名”，并在弹出的添加域名弹窗中填写域名信息。

单击“添加”可添加多个域名。

步骤 7 确认无误后，单击“确认”，完成添加。

----结束

删除域名组

⚠ 警告

删除域名组后无法恢复，请谨慎操作。

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤 5 切换至“域名组”页签，单击待删除的“操作”列的“删除”，在弹出的确认框中，输入“DELETE”，单击“确定”，完成删除。

如果需要删除网络域名组，则请在进入域名组页面后，选择“网络域名组”页签，并在网络型域名组页面中执行相应操作。

----结束

相关操作

- 导出域名组：单击列表上方的“导出”，选择需要的数据范围。
- 批量删除域名：在“域名组详情”界面，批量勾选域名后，单击列表上方的“删除”，确认无误后单击“确定”。
- 编辑域名组：单击目标所在行的名称，修改参数。
- 域名组在防护规则里设置后才会生效，添加防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 查看**网络域名组**类型解析出的 IP 地址：单击目标所在行的名称，进入“基本信息”页，单击域名列表中的“操作”列的“IP 地址”。

3.4.5.3 管理服务组

操作场景

服务组是多个服务（协议、源端口、目的端口）的集合。通过在访问规则中一键引用服务组，即可实现对特定对象群体的统一流量管控。此外，当服务组更新时会自动同步至所有关联策略，无需手动调整。这不仅能提升策略调整响应速度，还可以降低重复配置工作量，实现运维效率的全面提升。

约束与限制

- 添加自定义服务组和服务：
  - 每个服务组中最多添加 64 个服务成员。
  - 每个防火墙实例下最多添加 512 个服务组。
  - 每个防火墙实例下最多添加 900 个服务成员。
- 预定义服务组仅支持查看，不支持添加、修改、删除操作。
- 被防护规则引用的服务组不支持删除，需优先调整/删除对应规则。

添加自定义服务组

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中选择“访问控制 > 对象组管理”，进入对象组管理界面后，切换至“服务组”页签。

步骤 5 在自定义服务组页面中，单击“添加服务组”，并在弹出“添加服务组”界面中填写服务组信息。

表 3-55 添加服务组的参数说明

参数	说明

参数	说明
服务组名称	需要添加的服务组名称。
服务列表	• 协议：当前支持的协议为：TCP、UDP、ICMP。 • 源端口：设置需要开放或限制的源端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443 • 目的端口：设置需要开放或限制的目的端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443 • 描述：标识该服务组的使用场景和用途，以便后续运维时快速区分不同服务组的作用。
描述	标识该服务组的使用场景和用途，以便后续运维时快速区分不同服务组的作用。

步骤 6 确认填写信息无误后，单击“确认”，完成添加服务组。

服务组在防护规则里设置后才会生效，添加防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。

----结束

添加自定义服务组中服务

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3（可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中选择“访问控制 > 对象组管理”，进入对象组管理界面后，切换至“服务组”页签。

步骤 5 在自定义服务组页面中，单击目标服务组名称，弹出服务组详情页面。

步骤 6 单击“添加服务”，弹出添加服务页面后，填写服务信息。

表 3-56 添加服务

参数名称	参数说明	取值样例
协议	协议类型当前支持：TCP、UDP、ICMP。	TCP
源端口	设置需要开放或限制的源端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443。 协议选择 ICMP 时，无需填写端口号。	80

参数名称	参数说明	取值样例
目的端口	设置需要开放或限制的目的端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443。 协议选择 ICMP 时，无需填写端口号。	80
描述	标识该服务的使用场景和用途，以便后续运维时快速区分不同服务的作用。	-

步骤 7 如果需要添加多个服务，可单击“添加”进行处理。

步骤 8 确认无误后，单击“确认”，完成添加。

----结束

查看预定义服务组

云防火墙为您提供预定义服务组，包括常用 Web 服务、常用数据库和常用远程登录和 ping，适用于防护 Web、数据库和服务器。

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中选择“访问控制 > 对象组管理”，进入对象组管理界面后，切换至“服务组”页签。

步骤 5 选择“预定义服务组”页签，单击目标服务组的名称，进入详细信息页面，查看服务组信息。

----结束

删除自定义服务组

⚠ 警告

删除服务组后无法恢复，请谨慎操作。

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中选择“访问控制 > 对象组管理”，进入对象组管理界面后，切换至“服务组”页签。

步骤 5 在自定义服务组页面中，单击待删除的服务组所在行的“操作”列的“删除”。

步骤 6 在弹出删除确认框中，确认删除的信息无误后，输入“DELETE”，单击“确定”，完成删除。

----结束

相关操作

- 导出服务组：单击列表上方的“导出”，选择需要的数据范围。
- 批量删除服务：在“服务组详情”界面，批量勾选服务后，单击列表上方的“删除”，确认无误后，单击“确定”。

3.5 攻击防御

3.5.1 攻击防御功能概述

云防火墙的攻击防御功能支持防护网络攻击和病毒文件，建议您及时将 IPS 的“防护模式”切换至“拦截模式”。

前提条件

已开启至少一项流量防护：

- 开启 EIP 流量防护请参见 3.3.1 开启互联网边界流量防护。
- 开启 VPC 流量防护请参见 3.3.2 开启 VPC 边界流量防护。
- 开启私网 IP 流量防护请参见 3.3.3 开启 NAT 网关流量防护。

如何防御网络攻击和病毒文件

CFW 提供入侵防御 IPS、敏感目录扫描防御、反弹 Shell 检测防御、病毒防御 AV 功能防御网络攻击和病毒文件，具体介绍如表 3-57 所示。

表 3-57 攻击防御功能

功能	检测类型	配置指导

功能	检测类型	配置指导
入侵防御（IPS）	• 检查**威胁及漏洞扫描**； • 检测流量中是否含有**网络钓鱼、特洛伊木马、蠕虫、黑客工具、间谍软件、密码攻击、漏洞攻击、SQL 注入攻击、XSS 跨站脚本攻击、Web 攻击**； • 是否存在**协议异常、缓冲区溢出、访问控制、可疑 DNS 活动及其它可疑行为**。	调整 IPS 防护模式拦截网络攻击
敏感目录扫描防御	对云主机敏感目录的扫描攻击	开启敏感目录扫描防御
反弹 Shell 检测防御	通过反弹 Shell 方式进行的网络攻击	开启反弹 Shell 检测防御
病毒防御（AV）	通过病毒特征检测来识别和处理病毒文件，避免由病毒文件引起的数据破坏、权限更改和系统崩溃等情况发生，支持检测 HTTP、SMTP、POP3、FTP、IMAP4、SMB 的协议类型。	3.5.3 配置病毒防御

防护动作介绍

- 观察：不启用规则，防火墙对匹配当前规则的流量，记录至攻击事件日志中，不做拦截。
- 拦截：启用规则，防火墙对匹配当前规则的流量，记录至攻击事件日志中并进行拦截。
- 禁用：禁用规则，防火墙对匹配当前规则的流量，不记录、不拦截。

相关文档

整体防护概况请参见 3.5.4 通过安全看板查看攻击防御信息，详细日志信息请参见攻击事件日志。

3.5.2 配置入侵防御

云防火墙提供网络攻击防护，帮助您检测常见的网络攻击。

约束限制

- 入侵防御不支持对 TLS、SSL 加密的流量进行解密检测和防御。

对业务的影响

开启拦截模式后，入侵防御 IPS 功能会拦截各类威胁和恶意流量。建议您调整防护模式时，优先开启“观察模式”，等待业务运行一段时间排查误拦截后，再逐步更换至“拦截模式”。

入侵防御 IPS

入侵防御（IPS）功能结合多年攻防积累的经验规则，实时检测和防护访问流量，拦截多种常见的网络攻击，有效保护您的资产。

IPS 提供多类规则库：

- **基础防御**：内置的规则库，覆盖常见网络攻击，为您的资产提供基础的防护能力，您可以通过修改防护模式，调整规则库的防护状态，具体操作请参见调整 IPS 防护模式拦截网络攻击；如果需要调整单条规则的防护状态，请参见 3.5.5.1 修改入侵防御规则的防护动作。
- **虚拟补丁**：在网络层级为 IPS 提供热补丁，实时拦截高危漏洞的远程攻击行为，同时避免修复漏洞时造成业务中断。

  更新的规则优先进入虚拟补丁库中，您可以根据业务情况判断是否增加至基础防御库中。

  增加方式：打开开关，虚拟补丁中的规则将生效，实时防护并支持手动修改防护动作。
- **自定义 IPS 特征**（仅专业版支持）：提供的内置规则库无法满足需求时，支持自定义特征规则，请参见 3.5.5.2 自定义 IPS 特征。

  支持添加 HTTP、TCP、UDP、POP3、SMTP、FTP 协议类型的特征规则。

调整 IPS 防护模式拦截网络攻击

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入入侵防御界面。

步骤 5 保持“基础防御”右侧开关开启。

步骤 6 在“防护模式”栏中，选择合适的防护模式。

表 3-58 防护模式说明

防护模式	说明
观察模式	仅对攻击事件进行检测并记录到“攻击事件日志”中，不做拦截。

防护模式	说明
拦截模式	在发生明确攻击类型的事件和检测到异常 IP 访问时，将实施自动拦截操作。 • **拦截模式-宽松**：防护粒度较粗。拦截可信度高且威胁程度高的攻击事件。 • **拦截模式-中等**：防护粒度中等。满足大多数场景下的防护需求。 • **拦截模式-严格**：防护粒度精细，全量拦截攻击请求。
说明 • 建议您优先开启“观察模式”，等待业务运行一段时间后，再逐步更换至“拦截模式”，查看攻击事件日志，请参见攻击事件日志。 • 如果存在误拦截情况，可对基础防御规则库的单条防御规则进行动作修改，具体操作请参见 3.5.5 IPS 规则管理。	

不同防护模式会开启不同规则的拦截状态，对照表如表 3-59 所示，修改单条 IPS 规则请参见 3.5.5.1 修改入侵防御规则的防护动作。

表 3-59 规则组随防护模式变更的默认动作对照表

-	观察模式	拦截模式-严格	拦截模式-中等	拦截模式-宽松
“观察”规则组	观察	禁用	禁用	禁用
“严格”规则组	观察	拦截	禁用	禁用
“中等”规则组	观察	拦截	拦截	禁用
“宽松”规则组	观察	拦截	拦截	拦截

----结束

开启敏感目录扫描防御

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入入侵防御界面。

步骤 5 单击页面下方的“高级”按钮，并在“敏感目录扫描防御”模块，单击  ，启用防护。

- “动作”：
  - 观察模式：发现敏感目录扫描攻击后，仅记录至攻击事件日志。
  - 拦截 Session：发现敏感目录扫描攻击后，拦截当次会话。
  - 拦截 IP：发现敏感目录扫描攻击后，CFW 会阻断该攻击 IP 一段时间。

说明

配置“拦截 IP”后，CFW 会持续对 IP 进行阻断，如果涉及地址转换或者存在代理的场景，需要谨慎评估拦截 IP 的影响。

- “持续时长”：“动作”选择“拦截 IP”时，可设置阻断时间，范围为 60~3600s。
- “阈值”：对于单个敏感目录扫描频率达到设定的阈值后，CFW 会采取相应“动作”。

步骤 6 单击“确认”。

----结束

开启反弹 Shell 检测防御

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入入侵防御界面。

步骤 5 单击页面下方的“高级”按钮，并在“反弹 Shell 检测防御”模块，单击  ，启用防护。

- “动作”：
  - 观察模式：发现反弹 shell 攻击后，仅记录至攻击事件日志。
  - 拦截 Session：发现反弹 shell 攻击后，拦截当次会话。
  - 拦截 IP：发现反弹 shell 攻击后，CFW 会阻断该攻击 IP 一段时间。

说明

配置“拦截 IP”后，CFW 会持续对 IP 进行阻断，如果涉及地址转换或者存在代理的场景，需要谨慎评估拦截 IP 的影响。

- “持续时长”：“动作”选择“拦截 IP”时，可设置阻断时间，范围为 60~3600s。
- “模式”：
  - 低误报：防护粒度较粗，单次会话中攻击次数达到 4 次时触发观察或拦截，确保攻击处理没有误报。
  - 高检测：防护粒度精细，单次会话中攻击次数达到 2 次时触发观察或拦截，确保攻击能够及时被发现并处理。

步骤 6 单击“确认”。

----结束

后续操作

整体防护概况请参见 3.5.4 通过安全看板查看攻击防御信息，详细日志信息请参见攻击事件日志。

相关文档

IPS 误拦截的排查方式请参见 4.2.5 IPS 拦截了正常业务如何处理？。

3.5.3 配置病毒防御

本章节介绍如何开启病毒防御拦截病毒文件，以及如何修改病毒防御动作提升防护效果。

操作场景

当前病毒攻击日益复杂，传统杀毒方式难以及时应对。为提供更精准的防护，云防火墙的病毒防御（Anti-Virus，AV）功能通过病毒特征检测来识别和处理病毒文件，避免由病毒文件引起的数据破坏、权限更改和系统崩溃等情况发生，有效保护您的业务安全。

目前，云防火墙支持的病毒防御功能支持对 HTTP、SMTP、POP3、FTP、IMAP4、SMB 协议类型进行检测。

规格限制

仅专业版支持病毒防御功能。

开启病毒防御拦截病毒文件

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“攻击防御 > 病毒防御”，进入病毒防御页面。

步骤 5 单击  按钮，开启病毒防御功能。

开启病毒防御功能后，防火墙“当前动作”默认为“禁用”。如果需要修改防御动作，请参见修改病毒防御动作提升防护效果进行处理。

----结束

修改病毒防御动作提升防护效果

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“攻击防御 > 病毒防御”，进入病毒防御页面。

步骤 5 在防御规则列表中，单击目标防御规则“操作”列的相应按钮，选择对应动作。

- 观察：修改为“观察”状态，修改后防火墙对当前协议的流量进行检测，匹配到攻击流量时，记录至攻击事件日志中，不做拦截。
- 拦截：修改为“拦截”状态，修改后防火墙对当前协议的流量进行检测，匹配到攻击流量时，记录至攻击事件日志中并进行拦截。
- 禁用：修改为“禁用”状态，修改后防火墙对当前协议的流量不进行病毒检测。

----结束

后续操作

整体防护概况请参见 3.5.4 通过安全看板查看攻击防御信息，详细日志信息请参见攻击事件日志。

相关文档

- 攻击防御相关介绍请参见 3.5.1 攻击防御功能概述。
- 拦截网络攻击请参见 3.5.2 配置入侵防御。

3.5.4 通过安全看板查看攻击防御信息

操作场景

在日常的网络安全运维中，企业需要随时掌握流量的安全状态，云防火墙提供“安全看板”功能，支持快速查看 7 天内互联网入/出方向和 VPC 边界流量经过攻击防御功能（IPS、反弹 Shell、敏感目录扫描、病毒防御）的防护数据统计，便于您掌握流量的安全状态并及时调整防护配置。

约束限制

数据看板中的“攻击趋势”模块数据统计存在一定延时，且不同的查询时间段也取值方式不同，具体请参见表 3-60。如果需要查询实时数据，建议您通过“日志查询”进行查看，具体操作请参见 3.7 日志审计。

表 3-60 攻击趋势取值说明

时间段	取值
近 1 小时	取前 1 分钟内的平均值，按每分钟取整，例如 08:45:59 时查询，统计时取值的时间为 07:45:00~08:45:00。

时间段	取值
近 24 小时	取前 5 分钟内的平均值，按 5 分钟（5 的倍数）取整，例如 2025/06/30 08:48:59 时查询，统计时取值的时间为 2025/06/29 08:45:00~2025/06/30 08:45:00。
近 7 天	取前 1 小时内的平均值，按小时取整，例如 2025/06/30 08:45:59 时查询，统计时取值的时间为 2025/06/23 08:00:00~2025/06/30 08:00:00。
自定义	• 5 分钟~6 小时：取 1 分钟内的平均值，与“近 1 小时”取值方式一致。 • 6 小时（含）~3 天：取 5 分钟内的平均值，与“近 24 小时”取值方式一致。 • 3 天（含）~7 天（含）：取 30 分钟内的平均值，与“近 7 天”取值方式一致。

通过安全看板查看 IPS 防护信息

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“攻击防御 > 安全看板”，进入安全看板页面。

步骤 5 在页面上方，选择“互联网边界”或“VPC 边界”页签。

步骤 6 查看防火墙实例下攻击防御的统计信息，您可以在各模块右上角选择查询时间。

- 安全看板：IPS 检测到的攻击总数、放行/拦截的总数、被攻击的端口个数。
- 攻击趋势：IPS 阻断或放行的流量次数。
- 可视化统计：IPS 检测/拦截到的攻击参数 TOP 5 的排行，参数说明请参见表 3-61。单击单条数据查看攻击事件详情，参数说明请参见表 3-69。

表 3-61 安全看板可视化统计参数说明

参数名称	参数说明
攻击类型	攻击的类型。
TOP 内部攻击来源 IP	云内资产攻击外部 IP 时，云内资产的 IP。
TOP 外部攻击来源 IP	外部 IP 攻击云内资产时，外部的 IP。
TOP 外部攻击来源地区	外部 IP 攻击云内资产时，外部 IP 的来源地区。
TOP 攻击目的 IP	攻击事件中的目的 IP。

参数名称	参数说明
TOP 被攻击端口	攻击事件中受到攻击的端口。

- TOP 攻击统计：查看指定时间段内 IPS 检测/拦截中攻击次数 TOP 50 信息。
  - TOP 攻击来源统计：来源 IP、来源类型等信息。
  - TOP 攻击目的统计：目的 IP、目的端口、目的应用等信息。

说明

- 该 IP 地址是正常数据：单击“操作”列的“加白名单”，快速将该 IP 地址加入至白名单中，后续 CFW 将直接放行该 IP 地址的流量。
- 该 IP 地址是恶意攻击：单击“创建为地址组”或“添加到地址组”快速将多个 IP 地址添加至地址组中，添加后手动配置阻断的防护规则拦截恶意攻击，配置防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。

----结束

相关文档

- 详细日志信息请参见攻击事件日志。
- 攻击防御的防护能力请参见 3.5.1 攻击防御功能概述。
- IPS 误拦截的排查方式请参见 4.2.5 IPS 拦截了正常业务如何处理？。
- 调整 IPS 动作请参见 3.5.2 配置入侵防御，调整病毒防御动作请参见 3.5.3 配置病毒防御。

3.5.5 IPS 规则管理

3.5.5.1 修改入侵防御规则的防护动作

基础防御规则库和虚拟补丁规则库中的规则，支持手动修改防护动作，修改后，该规则将按照设置的动作进行执行，不再受 IPS“防护模式”的影响。

如果规则库中的防御规则不能满足您的需求，您可自定义 IPS 特征规则，请参见 3.5.5.2 自定义 IPS 特征。

约束条件

修改 IPS 规则存在以下限制：

- “防护模式”发生变化时，手动修改的规则“当前动作”保持不变。
- 当前动作修改条数限制如下。
  - 最多可修改 3000 条规则为“观察”。
  - 最多可修改 3000 条规则为“拦截”。
  - 最多可修改 128 条规则为“禁用”。

规则组随防护模式变更的默认动作对照表

-	观察模式	拦截模式-严格	拦截模式-中等	拦截模式-宽松
“观察”规则组	观察	禁用	禁用	禁用
“严格”规则组	观察	拦截	禁用	禁用
“中等”规则组	观察	拦截	拦截	禁用
“宽松”规则组	观察	拦截	拦截	拦截

说明

- 观察：不启用规则，防火墙对匹配当前规则的流量，记录至攻击事件日志中，不做拦截。
- 拦截：启用规则，防火墙对匹配当前规则的流量，记录至攻击事件日志中并进行拦截。
- 禁用：禁用规则，防火墙对匹配当前规则的流量，不记录、不拦截。

修改基础防御规则动作

当前动作修改条数限制如下：

- 最多可修改 3000 条规则为“观察”。
- 最多可修改 3000 条规则为“拦截”。
- 最多可修改 128 条规则为“禁用”。

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入入侵防御界面。

步骤 5 保持“基础防御”右侧开关开启。

步骤 6 单击“基础防御”栏中的“查看生效中的规则”，进入基础防御规则页面。

步骤 7 （可选）如需查看某类规则的参数详情，可在上方筛选输入框中，选择对应条件，筛选相关参数。

步骤 8 在基础防御规则列表中，单击目标规则“操作”列的对应动作。

如果您当前页面无“操作”列，需返回上一层并开启“基础防御”右侧开关。

- 观察：修改为“观察”状态，修改后防火墙对匹配当前防御规则的流量，记录至日志中，不做拦截。
- 拦截：修改为“拦截”状态，修改后防火墙对匹配当前防御规则的流量，记录至日志中并进行拦截。

- 禁用：修改为“禁用”状态，修改后防火墙对匹配当前防御规则的流量，不记录、不拦截。

修改后的防护规则，不随“防护模式”改变，如需恢复至**默认动作**，可以勾选需要恢复的规则，单击列表上方“恢复默认”。

----结束

相关文档

- 恢复部分规则的默认动作：在基础防御规则页面中，勾选规则，单击规则列表上方的“恢复默认”。
- 恢复全部规则的默认动作：在基础防御规则页面中，单击规则列表上方的“全局恢复默认”。
- 设置 IPS 的整体防护动作请参见 3.5.2 配置入侵防御。

3.5.5.2 自定义 IPS 特征

操作场景

在复杂多变的网络攻击面前，企业往往需要个性化的入侵检测方案，然而宽泛的特征规则容易引发大量误报，反而降低防护效率。为此，云防火墙支持为 HTTP、TCP、UDP、POP3、SMTP、FTP 协议添加精细化的自定义 IPS 特征规则，通过精准的签名特征匹配，有效识别恶意流量。

本章节介绍如何自定义 IPS 特征。配置时，**建议**设置具体的自定义特征，**避免**规则过宽导致误匹配和性能下降。

约束条件

- 仅“专业版”支持自定义 IPS 特征。
- 最多支持添加 500 条特征。
- 自定义的 IPS 特征不受修改基础防御防护模式的影响。
- 特征设置“方向”为“客户端到服务器”且“协议类型”为“HTTP”时，“内容选项”才能设置为“URI”。

添加自定义 IPS 特征

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入入侵防御页面后，单击“自定义 IPS 特征”栏中的“查看规则”，进入自定义 IPS 特征页面。

步骤 5 在“自定义 IPS 特征”页签中，单击列表左上角“添加自定义 IPS 特征”，并在添加自定义 IPS 规则页面中填写规则信息。

表 3-62 添加自定义 IPS 特征

参数名称	参数说明
名称	需要添加的特征名称。 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（-_）。 • 长度不能超过 255 个字符。
风险等级	设置特征的风险等级。
攻击类型	选择特征的攻击类型。
影响软件	选择受影响的软件。
操作系统	选择操作系统。
方向	选择该特征匹配流量的方向。 • Any：任意方向，符合其他条件的任意方向的流量都会匹配到当前规则。 • 服务器到客户端 • 客户端到服务器
协议类型	选择特征的协议类型。
源类型	选择源端口类型。 • Any：任意端口类型，等同于包含所有类型。 建议您优先选择“Any”。 • 包含 • 排除
源端口	“源类型”选择“包含”或“排除”时，设置源端口。 • 支持设置单个或多个端口，多个端口之间用半角逗号（,）隔开，如：80,100。 • 支持连续端口组，中间使用“-”隔开，如：80-443。
目的类型	选择目的端口类型。 • Any：任意端口类型，等同于包含所有类型。 建议您优先选择“Any”。 • 包含 • 排除
目的端口	“目的类型”选择“包含”或“排除”时，设置目的端口。 • 支持设置单个或多个端口，多个端口之间用半角逗号（,）隔开，如：80,100。 • 支持连续端口组，中间使用“-”隔开，如：80-443。

参数名称	参数说明
动作	防火墙检测到该特征流量时，采取的动作。 • 观察：仅对攻击事件进行检测并记录到日志中，日志记录查询请参见 3.7.2 日志查询。 • 拦截：实施自动拦截操作。 建议您优先选择“观察”，确认“攻击事件日志”记录正确后，再切换至“拦截”。
内容	特征规则中匹配的内容。 • 内容：跟特征匹配的内容字段，例如：cfw。 • 内容选项：选择“内容”匹配的限制规则。 – 十六进制：匹配十六进制时，“内容”需填写十六进制格式，例如：0x1F。 – 忽略大小写：匹配时不区分大小写。 – URL：匹配 URL 中跟“内容”一致的字段。 • 相对位置：匹配特征时，指定开始的位置。 – 头部：从报文“偏移”值的位置开始匹配特征，例如偏移：10，则该条内容从第 11 位开始。 **说明** 当“内容选项”选择“URL”时，头部的匹配位置从域名结束（包含端口）开始计算。 例如：www.example.com/test，偏移为 0，则该条内容从 com 后的/开始。 或 www.example.com:80/test，偏移为 0，则该条内容从 80 后的/开始。 – 上一个内容之后：报文中截取的位置从指定位置开始。 公式：上一条“内容”字段长度+上一条“偏移”值+“偏移”值+1 例如：上一条设置内容：test，偏移：10，本条偏移：5，则该条内容的匹配位置从第 20（4+10+5+1）位开始。 • 偏移：匹配特征时开始的位置，例如偏移：10，则代表该条内容的匹配位置从第 11 位开始。 • 深度：匹配特征时，截止匹配的位置，例如深度：65535，则代表该条内容的匹配位置到第 65535 位截止。 **说明** • “深度”值需大于“内容”字段长度。 • 一条 IPS 特征中最多添加 4 条内容。

步骤 6 单击“确认”，完成添加 IPS 特征。

----结束

相关文档

- 处理自定义 IPS 特征：
  - 复制自定义 IPS 特征：在目标特征所在行的“操作”列中，单击“复制”，修改参数信息后，单击“确认”，可以快速复制 IPS 特征。
  - 修改自定义 IPS 特征：在目标特征所在行的“操作”列中，单击“编辑”，可以修改 IPS 特征信息。修改完成后，单击“确认”。
  - 删除单个自定义 IPS 特征：在目标特征所在行的“操作”列中，单击“更多 > 删除”，并在弹出的确认框中单击“确定”。
  - 批量删除自定义 IPS 特征：勾选目标特征，单击列表上方的“删除”，并在弹出的确认框中单击“确定”，可以批量删除 IPS 特征。
  - 修改单个自定义 IPS 特征的动作：在目标特征所在行的“操作”列中，单击“更多 > 观察”或“更多 > 拦截”，可以修改防火墙的响应动作。
  - 批量修改自定义 IPS 特征的动作：勾选目标特征，单击列表上方的“观察”或“拦截”，可以批量修改防火墙的响应动作。
- 攻击防御相关介绍请参见 3.5.1 攻击防御功能概述。
- 拦截网络攻击请参见 3.5.2 配置入侵防御。

后续操作

整体防护概况请参见 3.5.4 通过安全看板查看攻击防御信息，详细日志信息请参见攻击事件日志。

3.6 流量分析

3.6.1 查看入云流量

入云流量页面展示当前防火墙实例防护的互联网访问云上 EIP 的流量数据。数据基于会话统计，在会话连接期间，数据不会上报，连接结束后才会上报。

前提条件

开启弹性公网 IP（EIP）防护且已有流量经过 EIP，开启 EIP 防护的操作步骤请参见 3.3.1 开启互联网边界流量防护。

查看入云流量

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“流量分析 > 入云流量”，进入入云流量页面。

步骤 5 查看经过防火墙的流量统计信息，支持 5 分钟~7 天的数据。

- 流量看板：互联网访问内部服务器时最大流量的相关信息。
- 入云流量：入方向请求流量和响应流量数据，最多支持同时查询 30 个 EIP 的流量数据。

  数据信息是流量日志中在该时间结束会话的流字节数的平均值。

表 3-63 取值说明

时间段	取值说明
近 1 小时	取 1 分钟内的平均值。
近 24 小时	取 5 分钟内的平均值。
近 7 天	取 1 小时内的平均值。
自定义	• 5 分钟~6 小时：取 1 分钟内的平均值。 • 6 小时（含）~3 天：取 5 分钟内的平均值。 • 3 天（含）~7 天（含）：取 30 分钟内的平均值。

- 可视化统计：查看指定时间段内入方向流量中指定参数的 TOP 5 排行，参数说明请参见表 3-64。单击单条数据查看流量详情，每个详情支持查看 50 条数据。

表 3-64 入云流量可视化统计参数说明

参数名称	参数说明
TOP 访问源 IP	入方向流量的源 IP 地址。
TOP 访问来源地区	入方向流量的源 IP 所属的地理位置。
TOP 访问目的 IP	入方向流量的目的 IP 地址。
TOP 开放端口	入方向流量的目的端口。
TOP 应用分布	入方向流量的应用信息。

- IP 分析：查看指定时间段内 TOP 50 的流量信息。
  - 公开 IP 分析：目的 IP 的流量信息。
  - 访问源 IP 分析：源 IP 的流量信息。

----结束

3.6.2 查看出云流量

出云流量页面展示当前防火墙实例防护的云上 EIP 访问互联网的流量数据，数据基于会话统计，在连接期间，数据不会上报，连接结束后才会上报。

前提条件

开启弹性公网 IP（EIP）防护且已有流量经过 EIP，开启 EIP 防护的操作步骤请参见 3.3.1 开启互联网边界流量防护。

规格限制

- “私网外联资产”数据查看需满足专业版防火墙且开启 VPC 边界防火墙防护，请参见 3.3.2 开启 VPC 边界流量防护。

查看出云流量

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“流量分析 > 出云流量”，进入出云流量页面。

步骤 5 查看经过防火墙的流量统计信息，支持 5 分钟~7 天的数据。

- 流量看板：内部服务器访问互联网时最大流量的相关信息。
- 出云流量：出方向请求流量和响应流量数据，最多支持同时查询 30 个 EIP 的流量数据。

  数据信息是流量日志中在该时间结束会话的流字节数的平均值。

表 3-65 取值说明

时间段	取值说明
近 1 小时	取 1 分钟内的平均值。
近 24 小时	取 5 分钟内的平均值。
近 7 天	取 1 小时内的平均值。
自定义	• 5 分钟~6 小时：取 1 分钟内的平均值。 • 6 小时（含）~3 天：取 5 分钟内的平均值。 • 3 天（含）~7 天（含）：取 30 分钟内的平均值。

- 可视化统计：查看指定时间段内出方向流量中指定参数的 TOP 5 排行，参数说明请参见表 3-66。单击单条数据查看流量详情，每个详情支持查看 50 条数据。

表 3-66 出云流量可视化统计参数说明

参数名称	参数说明
TOP 访问目的 IP	出方向流量的目的 IP 地址。

参数名称	参数说明
TOP 访问目的地区	出方向流量的目的 IP 所属的地理位置。
TOP 访问源 IP	出方向流量的源 IP 地址。
TOP 访问端口	出方向流量的目的端口。
TOP 应用分布	出方向流量的应用信息。

- IP 分析：查看指定时间段内 TOP 50 的流量信息。
  - 外联 IP：目的 IP 的流量信息。
  - 公网外联资产：源 IP 为公网 IP 的流量信息。
  - 私网外联资产：源 IP 为私网 IP 的流量信息。

说明

私网 IP 信息仅配置了 VPC 边界防护的专业版防火墙可见。

----结束

3.6.3 查看 VPC 间访问流量

VPC 间访问展示当前防火墙实例防护的 VPC 间流量数据。

前提条件

配置并开启 VPC 边界流量防护，且已有流量经过 VPC，开启 VPC 防护的操作步骤请参见 3.3.2 开启 VPC 边界流量防护。

查看 VPC 间访问流量

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“流量分析 >VPC 间访问”，进入 VPC 间访问页面。

步骤 5 查看经过云防火墙的流量统计信息，支持 5 分钟~7 天的数据。

- 流量看板：VPC 间最大流量的相关信息。
- VPC 间访问：VPC 间请求流量和响应流量数据。

  数据信息是流量日志中在该时间结束会话的流字节数的平均值。

表 3-67 取值说明

时间段	取值说明

时间段	取值说明
近 1 小时	取 1 分钟内的平均值。
近 24 小时	取 5 分钟内的平均值。
近 7 天	取 1 小时内的平均值。
自定义	• 5 分钟~6 小时：取 1 分钟内的平均值。 • 6 小时（含）~3 天：取 5 分钟内的平均值。 • 3 天（含）~7 天（含）：取 30 分钟内的平均值。

- 可视化统计：查看指定时间段内 VPC 间流量中指定参数的 TOP 5 排行，参数说明请参见表 3-68。单击单条数据查看流量详情，每个详情支持查看 50 条数据。

表 3-68 VPC 间流量可视化统计参数说明

参数名称	参数说明
TOP 访问源 IP	VPC 间流量的源 IP 地址。
TOP 访问目的 IP	VPC 间流量的目的 IP 地址。
TOP 开放端口	VPC 间流量的目的端口。
应用分布	VPC 间流量的应用信息。

- 私网 IP 活动明细：查看指定时间段内私网 IP 流量 TOP 50 信息。

----结束

3.7 日志审计

3.7.1 防护日志概述

本文介绍以下内容：

- 云防火墙提供的两种日志存储方式，请参见日志存储方式。
- 支持的日志类型，请参见日志类型。
- 日志中出现了异常拦截，排查方式请参见异常拦截排查。
- 将日志转储到 LTS 的操作指导日志管理使用方式。

日志存储方式

功能名称	存储时长	计费方式	接入方式	日志字段说明

功能名称	存储时长	计费方式	接入方式	日志字段说明
日志查询	7 天	免费	自动接入	3.7.2 日志查询
日志管理	1~365 天	按流量单独计费	需手动对接到 LTS 服务，具体操作请参见 3.7.3.1 配置日志。 更好的使用 LTS 日志功能，请参见日志管理使用方式。	3.7.3.3 日志字段说明

日志类型

云防火墙提供以下日志：

- 攻击事件日志：IPS 等攻击防御功能检测到的事件记录。
- 访问控制日志：命中访问控制策略的所有流量。
- 流量日志：查看通过防火墙的所有流量记录。

说明

安全云脑（SecMaster）支持一键接入 CFW 日志数据。如果接入的是新购买的 CFW 的日志数据，由于日志上报存在一定的延迟，因此，如果您当天在安全云脑执行了接入 CFW 日志操作，则将会隔天才能在在安全云脑中查看到上报的 CFW 日志数据。

异常拦截排查

- 访问控制日志出现异常拦截：可能是防护规则/黑名单/白名单配置有误，需检查策略配置，修改防护规则请参见 3.4.4.3 管理防护规则，修改黑白名单请参见编辑黑/白名单。
- 攻击事件日志出现异常拦截：可能是 IPS 当前的防护模式拦截了您的业务。
  - 如果是单个流量被拦截，可将被拦截的 IP 加入白名单。
  - 如果是多个流量被拦截，在日志中查看是被单个规则还是多个规则阻断。
    - 单个规则阻断：修改该规则的防护动作，请参见修改基础防御规则动作。
    - 多个规则阻断：修改当前的防护模式，请参见调整 IPS 防护模式拦截网络攻击。

日志管理使用方式

功能名称	功能描述	配置方式
配置日志	将日志对接 LTS，并创建日志组和日志流。	3.7.3.1 配置日志
更改存储时长	（可选）默认存储日志的时间为 7 天，存储时间可以在 1～365 天之间进行设置。	3.7.3.2 更改日志存储时长

功能名称	功能描述	配置方式
日志搜索与分析	（可选）通过合理的日志收集、高效的搜索方法和专业的分析工具，实现对系统或应用的全面监控和精细化管理。	请参见《云日志服务用户指南》中“日志搜索与分析”章节
日志可视化	（可选）将日志数据按照图表类型呈现。	请参见《云日志服务用户指南》中“日志搜索与分析”章节
配置告警规则	（可选）监控日志中的关键词，通过在一定时间段内，统计日志中关键字出现的次数，实时监控服务运行状态。	请参见《云日志服务用户指南》中“日志告警”章节
日志字段查看	介绍日志的中各个字段代表的含义。	3.7.3.3 日志字段说明

相关文档

- 访问控制策略的整体防护概况请参见 3.4.3 通过策略助手查看防护信息。
- 流量趋势的整体防护概况请参见 3.6 流量分析。
- 网络攻击防护的整体防护概况请参见 3.5.4 通过安全看板查看攻击防御信息

3.7.2 日志查询

云防火墙支持查询 7 天内的日志记录，为您提供三类日志：

- 攻击事件日志：IPS 等攻击防御功能检测到的事件记录。
- 访问控制日志：命中访问控制策略的所有流量。
- 流量日志：查看通过防火墙的所有流量记录。

将单类或者多类日志记录至 LTS 中，您可以查看 1-365 天的日志数据，请参见 3.7.3 日志管理。

约束条件

- 日志存储时长最多支持 7 天。
- 单类日志最多支持查看 10,00 条数据，导出 100,000 条记录。
- 流量日志基于会话统计，在连接期间，数据不会上报，须连接结束后才会上报。

攻击事件日志

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航树中，选择“日志审计 > 日志查询”，默认进入“攻击事件日志”页面，可查看近一周的攻击事件详细信息。

（可选）快速筛选日志数据：日志查询支持包含（默认）和不包含（勾选“排除”）两种搜索类型。

表 3-69 攻击事件日志参数说明

参数	说明
发生时间	攻击事件发生的时间。
攻击类型	攻击事件所属类型，主要包括：IMAP、DNS、FTP、HTTP、POP3、TCP、UDP 等。
危险等级	危险等级包括：严重、高、中、低。
规则 ID	对应规则的 ID 号。
规则名称	规则库中相对应的命中规则名称。
源 IP	攻击事件的来源 IP。 源 IP 为 WAF 回源 IP 时，“源 IP”会展示 WAF 回源 IP 和 RealIP，其中 RealIP 展示 X-Forwarded-For 对应的第一个 IP，即客户端的真实 IP。
标签	IP 类型标识。 • 其它标签：非 WAF 回源 IP，无需特别处理。 • WAF 回源 IP：“源 IP”是 WAF 回源 IP，如果本条记录的“响应动作”是阻断、阻断 IP、丢弃，需手动设置放行。 操作方式：根据“规则 ID”在 IPS 规则库中，在该规则的“操作”列，选择“观察”。
源国家/地区	攻击事件源 IP 所属的地理位置。
源端口	攻击事件的源端口。
目的 IP	攻击事件中受到攻击的 IP 地址。
目的国家/地区	攻击事件目的 IP 所属的地理位置。
目的端口	攻击事件的目的端口。
协议	攻击事件的协议类型。
应用	攻击事件的应用类型。
方向	包括两个方向：出方向、入方向。
响应动作	防火墙的动作，包括放行、阻断、阻断 IP、丢弃。

参数	说明
操作	查看：查看攻击事件的“基本信息”和“攻击 payload”。

----结束

访问控制日志

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航树中，选择“日志审计 > 日志查询”，进入日志查询页面后，选择“访问控制日志”页签，可查看近一周的访问控制流量详细信息。

如果需要修改指定 IP 访问控制的响应动作，请参照 3.4.2.1 通过防护规则拦截/放行流量或 3.4.2.5 通过黑白名单拦截/放行流量。

（可选）快速筛选日志数据：日志查询支持包含（默认）和不包含（勾选“排除”）两种搜索类型。

表 3-70 访问控制日志参数说明

参数	说明
命中时间	访问发生的时间。
源 IP	访问的源 IP 地址。
源国家/地区	访问源 IP 所属的地理位置。
源端口	访问控制的源端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
目的 IP	访问的目的 IP。
目的网址	访问的域名地址。
目的国家/地区	访问目的 IP 所属的地理位置。
目的端口	访问控制的目的端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
协议	访问控制的协议类型。
响应动作	包括观察者模式（“观察”）和拦截模式（“阻断”或“放行”）。
规则	访问控制的规则类型，包括黑名单、白名单。

----结束

流量日志

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航树中，选择“日志审计 > 日志查询”，选择“流量日志”页签，可查看近一周的流量字节数和报文数。

（可选）快速筛选日志数据：日志查询支持包含（默认）和不包含（勾选“排除”）两种搜索类型。

表 3-71 流量日志参数说明

参数	说明
开始时间	流量防护发生的时间。
结束时间	流量防护结束的时间。
源 IP	该条流量的源 IP 地址。
源国家/地区	访问源 IP 所属的地理位置。
源端口	该条流量的源端口。
目的 IP	访问的目的 IP。
目的网址	访问的域名地址。
目的国家/地区	访问目的 IP 所属的地理位置。
目的端口	该条流量的目的端口。
协议	该条流量的协议类型。
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。

----结束

相关文档

- 导出日志：单击日志列表右上角的 ，导出列表中的日志记录。

后续操作

- 访问控制日志出现异常拦截：可能是防护规则/黑名单/白名单配置有误，需检查策略配置，修改防护规则请参见 3.4.4.3 管理防护规则，修改黑白名单请参见编辑黑/白名单。
- 攻击事件日志出现异常拦截：可能是 IPS 当前的防护模式拦截了您的业务。
  - 如果是单个流量被拦截，可将被拦截的 IP 加入白名单。
  - 如果是多个流量被拦截，在日志中查看是被单个规则还是多个规则阻断。
    - 单个规则阻断：修改该规则的防护动作，请参见修改基础防御规则动作。
    - 多个规则阻断：修改当前的防护模式，请参见调整 IPS 防护模式拦截网络攻击。

3.7.3 日志管理

3.7.3.1 配置日志

您可以将攻击事件日志、访问控制日志、流量日志记录到云日志服务（Log Tank Service，简称 LTS）中，通过 LTS 记录的 CFW 日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。

LTS 对于采集的日志数据，通过海量日志数据的分析与处理，可以为您提供一个实时、高效、安全的日志处理能力。

⚠ 注意

- 防火墙支持通过“日志查询”查看并导出最近 7 天的日志数据，请参见 3.7.2 日志查询。
- LTS 按流量单独计费。

配置日志

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航树中，选择“日志审计 > 日志管理”，进入“日志管理”页面。开启对接云日志服务  。

步骤 5 创建日志组和日志流。操作步骤请参见“云日志服务 > 快速入门 > 创建日志组和日志流”。

为方便后续查看，建议您：

- 创建日志组时加入-cfw 为后缀。

- 创建日志流时分别为攻击事件日志、访问控制日志、流量日志加入-attack、-access、-flow 为后缀。

步骤 6 选择已创建的日志组和日志流。

选择日志组，开启并选择日志流。

- 攻击、访问、流量日志的格式均不一样，需配置不同的日志流分别记录。
  - 攻击日志：记录攻击告警信息，包括攻击事件类型、防护规则、防护动作、五元组、攻击 payload 等信息。
  - 访问日志：记录命中 ACL 策略的流量信息，包括命中时间、五元组、响应动作、访问控制规则等信息。
  - 流量日志：记录所有通过云防火墙的流量信息，包括开始时间、结束时间、五元组、字节数、报文数等信息。

步骤 7 单击“确定”，完成日志配置。

配置完成后，如果出现“您的权限不足”的提示，请授予“LTS FullAccess”权限。

----结束

3.7.3.2 更改日志存储时长

默认存储日志的时间为 7 天，存储时间可以在 1～365 天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS 提供转储功能，可以将日志转储至对象存储服务（OBS）中长期保存。

更改日志存储时长

步骤 1 已将日志转储至 LTS，操作步骤请参见 3.7.3.1 配置日志。

步骤 2 登录管理控制台。

步骤 3 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 5 在左侧导航树中，选择“日志审计 > 日志管理”，进入“日志管理”页面，单击“修改存储时长”。

- 支持 1-365 天存储，超出设置时长的日志会被自动删除。
- 存储时长越长，占用存储容量越大，如需转储至其它云服务中长期保存，请参见“云日志服务用户指南 > 日志转储”。
- 该页面如果出现“您的权限不足”的提示，请授予“LTS FullAccess”权限。

----结束

3.7.3.3 日志字段说明

本节介绍对接到 LTS 的日志字段。

攻击事件日志

字段	类型	描述
src_ip	string	源 IP 地址。
src_port	string	源端口号。
dst_ip	string	目的 IP 地址。
dst_port	string	目的端口号。
protocol	string	协议类型。
app	string	应用类型。
src_region_name	string	源地区名称。
src_region_id	string	源地区 ID。
dst_region_name	string	目的地区名称。
dst_region_id	string	目的地区 ID。
log_type	string	日志类型。 • internet：互联网边界流量日志 • nat：NAT 边界流量日志 • vpc：VPC 间流量日志
vsys	long	防火墙防护方向。 • 1：南北向 • 2：东西向
direction	string	流量方向。 • out2in：入方向 • in2out：出方向
action	string	防火墙当前的响应动作。 • permit：放行 • deny：阻断 • block：阻断 IP • drop：丢弃
packet	string	攻击日志的原始数据包。 **说明** 编码方式为 Base64 格式。
attack_rule	string	检测到攻击的防御规则。
attack_rule_id	string	检测到攻击的防御规则 ID 号。

字段	类型	描述
attack_type	string	发生攻击的类型。 • Vulnerability Exploit Attack：漏洞攻击 • Vulnerability Scan：漏洞扫描 • Trojan：木马病毒 • Worm：蠕虫病毒 • Phishing：网络钓鱼攻击 • Web Attack：Web 攻击 • Application DDoS：DDoS 攻击 • Buffer Overflow：缓冲区溢出攻击 • Password Attack：密码攻击 • Mail：邮件相关类型的攻击行为 • Access Control：访问控制行为 • Hacking Tool：黑客工具 • Hijacking：劫持行为 • Protocol Exception：存在异常协议 • Spam：存在垃圾邮件 • Spyware：存在间谍软件 • DDoS Flood：DDoS 泛洪攻击 • Suspicious DNS Activity：可疑 DNS 活动 • Other Suspicious Behavior：其它可疑行为
level	string	表示检测到威胁的等级。 • CRITICAL：严重 • HIGH：高 • MEDIUM：中 • LOW：低
source	string	检测到攻击的防御模式。 • 0：基础防御 • 1：虚拟补丁
event_time	long	检测到的攻击时间。

访问控制日志

字段	类型	描述

字段	类型	描述
rule_id	string	触发规则的 ID
src_ip	string	源 IP 地址。
src_port	string	源端口号。
dst_ip	string	目的 IP 地址。
dst_port	string	目的端口号。
src_region_name	string	源地区名称。
src_region_id	string	源地区 ID。
dst_region_name	string	目的地区名称。
dst_region_id	string	目的地区 ID。
log_type	string	日志类型。 • internet：互联网边界流量日志 • nat：NAT 边界流量日志 • vpc：VPC 间流量日志
dst_host	string	目的域名。
vsys	long	防火墙防护方向。 • 1：南北向 • 2：东西向
protocol	string	协议类型。
app	string	应用类型。
direction	string	流量方向。 • out2in：入方向 • in2out：出方向
action	string	防火墙当前的响应动作。 • permit：放行 • deny：阻断
hit_time	long	访问发生的时间。

流量日志

字段	类型	描述

字段	类型	描述
src_ip	string	源 IP 地址。
src_port	string	源端口号。
dst_ip	string	目的 IP 地址。
dst_port	string	目的端口号。
protocol	string	协议类型。
app	string	应用类型。
direction	string	流量方向。 • out2in：入方向 • in2out：出方向
action	string	防火墙当前的响应动作。 • permit：放行 • deny：阻断
src_region_name	string	源地区名称。
src_region_id	string	源地区 ID。
src_vpc	string	源 IP 地址所在 VPC 的 ID。
dst_region_name	string	目的地区名称。
dst_region_id	string	目的地区 ID。
dst_vpc	string	目的 IP 地址所在 VPC 的 ID。
log_type	string	日志类型。 • internet：互联网边界流量日志 • nat：NAT 边界流量日志 • vpc：VPC 间流量日志
dst_host	string	目的域名。
vsys	long	防火墙防护方向。 • 1：南北向 • 2：东西向
hit_time	long	访问发生的时间。
to_s_bytes	long	客户端向服务端发送的字节数。
to_c_bytes	long	服务端向客户端发送的字节数。

字段	类型	描述
to_s_pkts	long	客户端向服务端发送的报文数。
to_c_pkts	long	服务端向客户端发送的报文数。
bytes	long	防护流量的字节数。
packets	long	防护流量的报文数。
start_time	long	流开始时间
end_time	long	流结束时间

3.8 系统管理

3.8.1 告警通知

设置告警通知后，CFW 可将触发的告警信息通过您设置的接收通知方式（例如邮件或短信）发送给您，您可以及时监测防火墙状态，迅速获得异常情况。

CFW 支持设置以下告警：

- 攻击告警：IPS 检测到攻击时触发告警。
- 流量超额预警：当流量达到所采购流量处理能力规格的一定比例时触发告警。
- EIP 未防护告警：当前账号有未开启防护的 EIP 时触发告警。

攻击告警

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 告警通知”，进入告警通知页面。

步骤 5 在“攻击告警”所在行的“操作”列，单击“编辑”，并在弹出的通知项设置页面中，设置通知项参数。

说明

通知设置修改后即时生效。

表 3-72 攻击告警参数说明

参数名称	参数说明
通知项说明	IPS 攻击日志告警。

参数名称	参数说明
通知等级	选择触发通知的危险等级。 可选择“致命”、“高”、“中”、“低”，支持多选。 例如：选择“高”和“中”，那么当防火墙检测到危险等级为高和中的入侵时，CFW 将以短信或邮件的方式通知您及时处理。
通知时间	选择通知的时间段。 在告警通知时间段内发现异常时，CFW 会在该告警时间段内发送相关通知；如果在告警时间段外发现异常，则不会发送通知。
触发条件	设置触发条件。 在设置时间间隔内，当攻击次数大于或等于您设置的阈值时系统才会发送告警通知。
通知群组	单击下拉列表选择已创建的主题，用于配置接收告警通知的终端。

步骤 6 单击“确认”，完成通知项设置。

步骤 7 确认信息无误后，在“攻击告警”所在行的“生效状态”列，单击 ，开启攻击告警通知。

----结束

流量超额预警

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 告警通知”，进入告警通知页面。

步骤 5 在“流量超额预警”所在行的“操作”列，单击“编辑”，并在弹出的通知项设置页面中，设置通知项参数。

说明

通知设置修改后即时生效。

表 3-73 流量超额预警参数说明

参数名称	参数说明
通知项说明	当流量达到所采购流量处理能力规格的一定比例时，发送告警通知。

参数名称	参数说明
通知等级	选择触发通知的流量等级，当流量（出流量或入流量的最大峰值）达到采购流量的该比例时，触发告警通知。 在下拉框中选择触发通知的流量占比等级，可选择“70%”、“80%”、“90%”。 例如：选择“80%”，那么当所用流量/购买流量=80%时，发送告警通知。
通知时间	选择通知的时间段。 在告警通知时间段内发现异常时，CFW 会在该告警时间段内发送相关通知；如果在告警时间段外发现异常，则不会发送通知。
触发条件	一天一次。
通知群组	单击下拉列表选择已创建的主题，用于配置接收告警通知的终端。

步骤 6 单击“确认”，完成通知项设置。

步骤 7 确认信息无误后，在“流量超额预警”所在行的“生效状态”列，单击 ，开启流量超额预警通知。

----结束

EIP 未防护告警

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 告警通知”，进入告警通知页面。

步骤 5 在“EIP 未防护告警”所在行的“操作”列，单击“编辑”，并在弹出的通知项设置页面中，设置通知项参数。

说明

通知设置修改后即时生效。

表 3-74 EIP 未防护告警参数说明

参数名称	参数说明
通知项说明	当前账号存在未开启防护的 EIP 时，发送告警通知。

参数名称	参数说明
通知时间	选择通知的时间段。 在告警通知时间段内发现异常时，CFW 会在该告警时间段内发送相关通知；如果在告警时间段外发现异常，则不会发送通知。
触发条件	一天一次。
通知群组	单击下拉列表选择已创建的主题，用于配置接收告警通知的终端。

步骤 6 单击“确认”，完成通知项设置。

步骤 7 确认信息无误后，在“EIP 未防护告警”所在行的“生效状态”列，单击  ，开启 EIP 防护通知。

----结束

相关文档

EIP 未开启防护白名单：在目标所在行的“操作”列，单击“添加告警白名单”，勾选 EIP 添加至右侧列表中，单击“确认”，该 EIP 未开启防护时，将不会发送告警通知。

图 3-17 添加告警白名单

3.8.2 DNS 服务器配置

操作场景

DNS（Domain Name System，域名系统）服务器用于将域名转换为 IP 地址，是网络通信的关键组件。云防火墙使用设置的默认 DNS 服务器进行域名解析。如果默认 DNS 无法满足您的需求，或者您的业务系统依赖其他 DNS 服务器来解析域名，您可以更换默认 DNS 服务器，或自定义指定 DNS 服务器地址。设置完成后，域名防护策略将根据您配置的 DNS 服务器进行 IP 解析并下发。

此外，当您的账号存在多个防火墙时，DNS 解析操作仅应用于当前操作的防火墙。

本章节介绍如何更换默认 DNS 服务器或自定义 DNS 服务器。

约束条件

最多支持自定义 2 个 DNS 服务器。

DNS 服务器配置

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3（可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 >DNS 配置”，进入 DNS 配置页面。

步骤 5 选择“默认 DNS 服务器”或添加“指定 DNS 服务器”。

说明

当前仅支持添加 2 个指定 DNS 服务器地址。

步骤 6 配置完成后，单击“应用”。

当前账号拥有多个防火墙时，DNS 解析操作仅应用于设置的防火墙。

----结束

后续操作

完成 DNS 服务配置后需添加防护规则，请参见 3.4.2 配置访问控制策略。

3.8.3 安全报告管理

3.8.3.1 安全报告概述

云防火墙提供安全报告，支持以日报、周报或自定义周期报告的形式，统计并展示用户已防护资产的安全趋势和关键事件、风险。

约束限制

- 安全报告仅保留 3 个月，建议您定期下载，以满足等保测评以及审计的需要。

安全报告使用说明

报告生成后，报告内容和生成时间如下：

- 报告内容：
  - 安全事件详情：当前入侵防御状态、事件等级分布、安全事件趋势、TOP 外部攻击来源 IP、TOP 攻击目的 IP、攻击类型、事件 TOP 攻击分布

  - 互联网边界防火墙：
    - 访问控制策略、资产管理、威胁事件、流量峰值
    - 弹性公网 IP 防护统计、流量趋势
    - 统计周期内，云防火墙管理 EIP 资产、访问控制策略、威胁事件和流量峰值具体信息
    - 入云流量：TOP 访问源 IP、TOP 访问目的 IP、TOP 访问端口
    - 出云流量：TOP 访问源 IP、TOP 访问域名、TOP 开放端口
  - VPC 边界防火墙：VPC 防护情况、规则数量、 VPC 间流量分析
    - 访问控制策略、资产管理、威胁事件、流量峰值
    - VPC 间防护统计、流量趋势
    - 统计周期内，云防火墙管理 VPC 资产、访问控制策略、威胁事件和流量峰值具体信息
    - TOP 访问目的 IP、TOP 访问源 IP、TOP 应用分布
- 报告生成时间：
  - 安全日报

    统计周期：每天 00:00:00 ~ 24:00:00

    报告将在生成后的次日自动发送至您设置的报告接收人。
  - 安全周报

    统计周期：周一 00:00:00 ~ 周日 24:00:00

    报告将在生成后的指定时间自动发送至您设置的报告接收人。
  - 自定义报告：自定义选择时间范围。

    统计周期：您可自定义安全报告统计的时间范围

    报告将会在创建成功一段时间后生成，生成后会自动发送至您设置的报告接收人。

您可以根据需要创建安全报告，详细操作请参见 3.8.3.2 创建安全报告。

报告生成后，您可以查看安全报告，详细操作请参见 3.8.3.3 查看/下载安全报告。

3.8.3.2 创建安全报告

您可以通过获取安全报告，及时掌握资产的安全状况数据。CFW 将按照设置的时间段以及接收方式将日志报告发送给您。

本节介绍如何创建安全报告。

约束限制

- 单个防火墙实例中，最多可创建 10 个安全报告。
- 安全报告仅保留 3 个月，建议您定期下载，以满足等保测评以及审计的需要。
- 自定义报告不支持修改，如需修改可删除后重新创建。

创建安全报告

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 安全报告”，进入安全报告页面。

步骤 5 单击“创建新模板”，进入创建新模板页面，配置报告参数信息。

表 3-75 安全报告模板参数说明

参数名称	参数说明
报告名称	自定义安全报告名称。
报告类型	• 安全日报 统计周期：每天 00:00:00 ~ 24:00:00 报告将在生成后的次日自动发送至您设置的报告接收人。 • 安全周报 统计周期：周一 00:00:00 ~ 周日 24:00:00 报告将在生成后的指定时间自动发送至您设置的报告接收人。 • 自定义报告：自定义选择时间范围。 统计周期：您可自定义安全报告统计的时间范围 报告将会在创建成功一段时间后生成，生成后会自动发送至您设置的报告接收人。
统计周期	“报告类型”选择“自定义报告”时，需要配置日志统计周期。
报告发送时间	当“报告类型”选择为“日报”、“周报”时，需要设置报告发送时间点，默认发送上一个统计周期的日志报告。 **说明** • 为了保证正确性，报告发送时间可能存在延迟。 • “报告类型”选择为“自定义报告”时，生成后自动发送。
通知群组	单击下拉列表选择已创建的主题，用于配置接收日志报告的终端。

步骤 6 单击“确认”，安全报告创建完成。

----结束

后续操作

下载并查看安全报告请参见 3.8.3.3 查看/下载安全报告。

相关文档

需要开启/关闭、修改、删除安全报告请参见 3.8.3.4 管理安全报告。

3.8.3.3 查看/下载安全报告

本节介绍如何查看已创建的安全报告及其展示的信息。

查看/下载最新安全报告

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 安全报告”，进入安全报告页面。

步骤 5 单击目标报告的“获取最新报告”，跳转至“安全报告预览”页，可查看报告信息。

步骤 6 如需下载，可在安全报告预览页面中，单击右下角的“下载”，可获取报告。

----结束

查看/下载历史安全报告

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 安全报告”，进入安全报告页面。

步骤 5 单击目标报告的“历史报告”，弹出“历史报告”，可查看报告列表。

步骤 6 单击“操作”列的“获取报告”，可查看报告信息。

步骤 7 如需下载，可在安全报告预览页面中，单击右下角的“下载”，可获取报告。

----结束

3.8.3.4 管理安全报告

本节介绍如何管理安全报告，包括开启、关闭、修改、删除操作。

约束限制

- 安全报告仅保留 3 个月，建议您定期下载，以满足等保测评以及审计的需要。
- 自定义报告不支持修改，如需修改可删除后重新创建。

开启/关闭安全报告

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 安全报告”，进入安全报告页面。

步骤 5 单击目标报告右上角的按钮切换状态。

-  ：当前已开启
-  ：当前已关闭

----结束

修改安全报告

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 安全报告”，进入安全报告页面。

步骤 5 单击目标报告右下角的“编辑” ，修改报告信息。

表 3-76 安全报告模板参数说明

参数名称	参数说明
报告名称	安全报告的名称。
报告类型	• 安全日报 统计周期：每天 00:00:00 ~ 24:00:00 报告将在生成后的次日自动发送至您设置的报告接收人。 • 安全周报 统计周期：周一 00:00:00 ~ 周日 24:00:00 报告将在生成后的指定时间自动发送至您设置的报告接收人。
报告发送时间	当“报告类型”选择为“日报”、“周报”时，需要设置报告发送时间点，默认发送上一个统计周期的日志报告。

参数名称	参数说明
通知群组	单击下拉列表选择已创建的主题，用于配置接收日志报告的终端。

步骤 6 单击“确认”，安全报告修改完成。

----结束

删除安全报告

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“系统管理 > 安全报告”，进入安全报告页面。

步骤 5 单击目标报告右下角的“删除”，删除报告信息。

----结束

3.9 使用 CES 监控 CFW

3.9.1 CFW 监控指标说明

功能说明

本节定义了云防火墙上报云监控服务的监控指标的命名空间和监控指标列表，用户可以通过云监控服务提供管理控制台来检索云防火墙产生的监控指标和告警信息。

命名空间

SYS.CFW

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

监控指标

表 3-77 是旧版指标，建议优先使用表 3-78 中指标。

表 3-77 云防火墙服务支持的监控指标（不建议使用）

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
used_protection_bandwidth	防护带宽使用量	该指标用于统计近 5 分钟内 CFW 检测到的互联网带宽使用量。	≥ 0 值类型：Float	KB/s	1000(SI)	云防火墙	5 分钟
protection_bandwidth_usage	防护带宽使用率	该指标用于统计 5 分钟内 CFW 检测到的互联网带宽使用率。 采集方式：带宽使用量/防火墙带宽配额的占比。	≥ 0 值类型：Float	百分比	不涉及	云防火墙	5 分钟

表 3-78 云防火墙服务支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
internet_protection_bandwidth_usage	互联网防护带宽使用量	该指标为防火墙互联网防护对象带宽使用量。	≥ 0 值类型：Float	Bit/s	1000(SI)	云防火墙	每分钟
vpc_protection_bandwidth_usage	VPC 间防护带宽使用量	该指标为防火墙 VPC 间防护对象带宽使用量。	≥ 0 值类型：Float	Bit/s	1000(SI)	云防火墙	每分钟
internet_protection_bandwidth_usage_rate	互联网防护带宽使用率	该指标为防火墙互联网防护对象带宽使用率。	≥ 0 值类型：Float	%	不涉及	云防火墙	每分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
vpc_protection_bandwidth_usage_rate	VPC 间防护带宽使用率	该指标为防火墙 VPC 间防护对象带宽使用率。	≥ 0 值类型：Float	%	不涉及	云防火墙	每分钟
internet_protection_pps	防火墙互联网方向 pps	该指标为防火墙互联网防护对象 pps。	≥ 0 值类型：Float	个	不涉及	云防火墙	每分钟
vpc_protection_pps	防火墙 VPC 间 pps	该指标为防火墙 VPC 间防护对象 pps。	≥ 0 值类型：Float	个	不涉及	云防火墙	每分钟
ips_hit_count	IPS 规则命中次数	该指标为流量命中 IPS 规则的次数。	≥ 0 值类型：Int	次	不涉及	云防火墙	每分钟
ips_deny_count	IPS 规则阻断次数	该指标为流量被 IPS 规则阻断的次数。	≥ 0 值类型：Int	个	不涉及	云防火墙	每分钟
acl_hit_count	ACL 规则命中次数	该指标为流量命中 ACL 规则的次数。	≥ 0 值类型：Int	个	不涉及	云防火墙	每分钟
acl_deny_count	ACL 规则阻断次数	该指标为流量被 ACL 模块阻断的次数。	≥ 0 值类型：Int	个	不涉及	云防火墙	每分钟
internet_protection_bandwidth_usage_inbound	入网防护带宽	该指标为防火墙互联网防护对象入方向带宽大小。	≥ 0 值类型：Float	Bit/s	1000(SI)	云防火墙	每分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
internet_protection_bandwidth_usage_outbound	出网防护带宽	该指标为防火墙互联网防护对象出方向带宽大小。	≥ 0 值类型：Float	Bit/s	1000(SI)	云防火墙	每分钟
internet_protection_bandwidth_usage_rate_inbound	入网防护带宽使用率	该指标为防火墙互联网防护对象入方向带宽/互联网边界防护带宽。	≥ 0 值类型：Float	%	不涉及	云防火墙	每分钟
internet_protection_bandwidth_usage_rate_outbound	出网防护带宽使用率	该指标为防火墙互联网防护对象带宽出方向使用率。	≥ 0 值类型：Float	%	不涉及	云防火墙	每分钟
internet_protection_pps_inbound	入网pps	该指标为访问防火墙互联网防护对象 pps。	≥ 0 值类型：Float	个	不涉及	云防火墙	每分钟
internet_protection_pps_outbound	出网pps	该指标为防火墙互联网防护对象访问外网pps。	≥ 0 值类型：Float	个	不涉及	云防火墙	每分钟

维度

Key	Value
fw_instance_id	防火墙 ID

3.9.2 设置监控告警规则

通过设置 CFW 告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解 CFW 防护状况，从而起到预警作用。

设置监控告警规则

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“管理与监管 > 云监控服务 ”。

步骤 3 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤 4 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤 5 根据界面提示配置参数，关键参数如下，更多参数信息请参见《云监控服务用户指南》的“创建告警规则和通知”章节：

- 告警类型：指标
- 资源类型：云防火墙
- 维度：云防火墙实例

步骤 6 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

3.9.3 查看监控指标

您可以通过管理控制台，查看 CFW 的相关指标，及时了解云防火墙防护状况，并通过指标设置防护策略。

查看监控指标

步骤 1 在云监控页面设置 CFW 的监控告警规则。有关设置监控告警规则的详细操作，请参见 3.9.2 设置监控告警规则。

步骤 2 在“云监控服务”的左侧导航树栏中，选择“云服务监控 > 云防火墙”，进入云服务监控详情页面。

步骤 3 在目标 CFW 实例所在行的“操作”列中，单击“查看监控指标”，查看对象的指标详情。

----结束

3.10 使用 CTS 审计 CFW 操作事件

3.10.1 支持云审计的 CFW 操作列表

云审计服务（Cloud Trace Service，CTS）记录了云防火墙相关的操作事件，方便用户日后的查询、审计和回溯。

云审计服务支持的 CFW 操作列表如表 3-79 所示。

表 3-79 云审计服务支持的 CFW 操作列表

操作名称	资源类型	事件名称
EIP 防护操作	eip_protection_operation	eipOperateProtectService
EIP 防护开启	eip_protection_operation	eipOperateProtectServiceEnable
EIP 防护关闭	eip_protection_operation	eipOperateProtectServiceDisable
创建 ACL 规则	acl	createACLRule
修改 ACL 规则	acl	createACLRule
删除 ACL 规则	acl	deleteACLRule
设置 ACL 规则优先级	acl	modifyACLRule
查看 ACL 规则命中次数 **说明** 此处的命中次数为策略列表中的命中次数，除非手动清零否则将会一直累计。	acl	showRuleHitCount
设置 ACL 优先级	acl	setACLRulePriority
创建黑名单	black_white_list	createBlackList
修改黑名单	black_white_list	modifyBlackList
删除黑名单	black_white_list	deleteBlackList
创建白名单	black_white_list	createWhiteList
修改白名单	black_white_list	modifyWhiteList
删除白名单	black_white_list	deleteWhiteList
新建 IP 地址组	address_group	createIPAddressGroup
更新 IP 地址组	address_group	updateIPAddressGroup
删除 IP 地址组	address_group	deleteIPAddressGroup
批量删除地址组	address_group	batchDeleteIPAddressGroup

操作名称	资源类型	事件名称
添加 IP 地址组成员	address_group_member	addIPAddressGroupMember
更新 IP 地址组成员	address_group_member	updateIPAddressGroupMember
删除地址组成员	address_group_member	deleteIPAddressGroupMember
新建服务组	service_group	addServiceGroup
更新服务组	service_group	updateServiceGroup
删除服务组	service_group	deleteServiceGroup
批量删除服务组	service_group	batchDeleteServiceGroup
添加服务组成员	service_group_member	addServiceGroupMember
更新服务组成员	service_group_member	updateServiceGroupMember
删除服务组成员	service_group_member	deleteServiceGroupMember
新建域名组	domain_set	addDomainSet
更新域名组	domain_set	updateDomainSet
删除域名组	domain_set	deleteDomainSet
批量删除域名组	domain_set	batchDeleteDomainSet
批量添加域名	domain_set	batchAddDomain
删除域名	domain	deleteDomainName
创建时间计划	schedule	createSchedule
更新时间计划	schedule	updateSchedule
删除时间计划	schedule	deleteSchedule
批量删除时间计划	schedule	batchDeleteSchedule
创建抓包任务	capture	createCaptureTask
截止抓包任务	capture	deleteCaptureTask
删除抓包任务	capture	cancelCaptureTask
创建东西向防火墙	cfw	createEWFirewallInstance
创建南北向防火墙	cfw	createSNFirewallInstance
更新防火墙	cfw	updateFirewallInstance
删除防火墙	cfw	deleteFirewallInstance

操作名称	资源类型	事件名称
升级防火墙	cfw	upgradeFirewallInstance
新增标签	cfw	createTags
删除标签	cfw	deleteTags
冻结防火墙 **说明** 防火墙可能因以下原因处于冻结状态： • 账号欠费。 • 账号冻结，例如账号违规。	cfw	freezeFirewallInstance
修改防火墙名称	cfw	changeFirewallName
更新攻击日志下发配置信息	alarm_config	updateAlarmConfig
更新用户的域名服务器配置情况	dns_server	updateDnsServer
创建东西向墙	cfw	createEastWestFirewall
东西向墙开启防护	cfw	enableEwFirewallProtect
东西向墙关闭防护	cfw	disableEwFirewallProtect
购买防火墙	cfw	addFirewallOrder
删除防火墙任务	cfw	deleteFirewall
升级防火墙任务	cfw	changeFirewall
ips 防护模式修改/创建	ips	createOrUpdateIpsMode
开启虚拟补丁	ips	enableVirtualPatches
关闭虚拟补丁	ips	disableVirtualPatches
修改敏感目录扫描状态或反弹 shell 规则状态	cfw	changeAdvanceIpsRuleStatus
修改日志管理	log_config	changeLogConfig
导入 ACL	import	importCFW

3.10.2 在 CTS 事件列表查看云审计事件

场景描述

云审计服务能够为您提供云服务资源的操作记录，记录的信息包括发起操作的用户身份、IP 地址、具体的操作内容的信息，以及操作返回的响应信息。根据这些操作记录，您可以很方便地实现安全审计、问题跟踪、资源定位，帮助您更好地规划和利用已有资源、甄别违规或高危操作。

什么是事件

事件即云审计服务追踪并保存的云服务资源的操作日志，操作包括用户对云服务资源新增、修改、删除等操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。

约束与限制

- 用户通过云审计控制台只能查询最近 7 天的操作记录，过期自动删除，不支持人工删除。如果需要查询超过 7 天的操作记录，您必须配置转储到对象存储服务（OBS）或云日志服务（LTS），才可在 OBS 桶或 LTS 日志组里面查看历史事件信息。否则，您将无法追溯 7 天以前的操作记录。
- 用户对云服务资源做出创建、修改、删除等操作后，1 分钟内可以通过云审计控制台查询管理类事件操作记录，5 分钟后才可通过云审计控制台查询数据类事件操作记录。

查看审计事件

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对 OBS 桶中数据的操作。云审计服务管理控制台会保存最近 7 天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近 7 天的操作记录。

在 CTS 查看审计事件

步骤 1 登录控制台，单击左上角 ☰，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。

步骤 2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤 3 在页面右上方，可以通过筛选时间范围，查询最近 1 小时、最近 1 天、最近 1 周的操作事件，也可以自定义最近 7 天内任意时间段的操作事件。

步骤 4 事件列表支持通过筛选来查询对应的操作事件。

表 3-80 事件筛选参数说明

参数名称	说明

参数名称	说明
事件类型	事件类型分为“管理事件”和“数据事件”。 • 管理类事件，即用户对云服务资源新建、修改、删除等操作事件。 • 数据类事件，即 OBS 服务上报的 OBS 桶中的数据的操作事件，例如上传数据、下载数据等。
云服务	在下拉选项中，选择触发操作事件的云服务名称。
资源类型	在下拉选项中，选择操作事件涉及的资源类型。 支持的资源类型请参见“支持云审计的 CFW 操作列表”章节。
筛选类型	筛选类型分为“资源 ID”、“事件名称”和“资源名称”。 • 资源 ID：操作事件涉及的云资源 ID。 当该资源类型无资源 ID，或资源创建失败时，该字段为空。 • 事件名称：操作事件的名称。 支持审计的操作事件的名称请参见“支持云审计的 CFW 操作列表”章节。 • 资源名称：操作事件涉及的云资源名称。 当事件所涉及的云资源无资源名称，或对应的 API 接口操作不涉及资源名称参数时，该字段为空。
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的 trace_type 的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。
事件级别	可选项包含“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。 • Normal 代表操作成功。 • Warning 代表操作失败。 • Incident 代表比操作失败更严重的情况，如引起其他故障等。

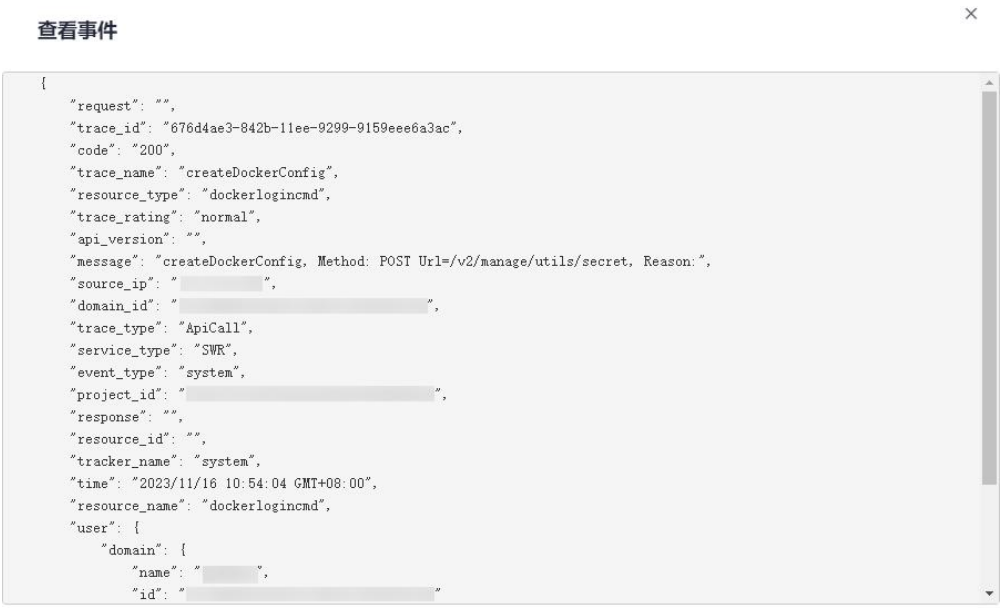
步骤 5 选择完查询条件后，单击“查询”。

步骤 6 在事件列表页面，您还可以导出操作记录文件和刷新列表。

- 单击“导出”按钮，云审计服务会将查询结果以 CSV 格式的表格文件导出，该 CSV 文件包含了本次查询结果的所有事件，且最多导出 5000 条信息。
- 单击按钮，可以获取到事件操作记录的最新信息。

步骤 7 在需要查看的事件左侧，单击 展开该记录的详细信息。

步骤 8 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



----结束

相关文档

- 关于事件结构的关键字段详解，请参见“《云审计服务用户指南》 > 事件参考 > 事件结构”章节和“《云审计服务用户指南》 > 事件参考 > 事件样例”章节。

4 常见问题

4.1 产品咨询

4.1.1 云防火墙支持线下服务器吗？

不支持，云防火墙支持云上 region 级服务。

4.1.2 云防火墙支持防护哪些范围？

云防火墙是新一代的云原生防火墙，支持防护的范围如下：

- 互联网边界：支持防护 EIP 的流量，包括入方向（从互联网到防火墙）和出方向（从防火墙到互联网）的流量。
- VPC 边界：支持防护 VPC 与 VPC 之间、云上 VPC 与本地 IDC 之间的流量；不支持防护 VPC 内的流量。
- NAT 网关分为以下两种场景：
  - 防护 NAT 网关绑定的 EIP，仅审计 EIP 的流量。
  - 防护 SNAT 和 DNAT 流量（依赖 VPC 边界防火墙），支持溯源到私网 IP。

4.1.3 云防火墙支持的 QPS、新建/并发连接数大小是多少？

云防火墙作为 SaaS 化服务，不受传统硬件防火墙在新建连接数、并发连接数以及 QPS 等方面的限制，衡量云防火墙性能的唯一标准是实际的防护带宽大小。

防护带宽定义如下：

- 防护带宽：所有经过云防火墙防护的业务带宽。
- 互联网边界防护带宽：所有经过云防火墙防护的 EIP 的流量总和最大值，按照入云流量（入流量）或出云流量（出流量）的最大值取值。
- VPC 边界防护带宽：所有经过云防火墙防护的 VPC 的流量总和最大值。

4.1.4 云防火墙支持跨账号使用吗？

云防火墙不支持跨账号使用。用户仅能使用并管理当前账号下的云防火墙资源。

4.1.5 云防火墙与 Web 应用防火墙有什么区别？

云防火墙和 Web 应用防火墙是两款不同的产品，为您的互联网边界和 VPC 边界、Web 服务提供防护。

WAF 和 CFW 的主要区别说明如表 4-1 所示。

表 4-1 CFW 和 WAF 的主要区别说明

类别	云防火墙	Web 应用防火墙
定义	云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和 VPC 边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持 AI 提升智能防御能力满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	Web 应用防火墙（Web Application Firewall，WAF），通过对 HTTP(S)请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定。
防护对象	• 弹性公网 IP 和 VPC 边界。 • 支持对 Web 攻击的基础防护。 • 支持外部入侵和主动外联的流量防护。	• 针对域名或 IP，云上或云下的 Web 业务。 • 支持对 Web 攻击的全面防护。
功能特性	• 资产管理与入侵防御：对已开放公网访问的服务资产进行安全盘点，进行实时入侵检测与防御。 • 访问控制：支持互联网边界访问流量的访问控制。 • 流量分析与日志审计：VPC 间流量全局统一访问控制，全流量分析可视化，日志审计与溯源分析。	SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击防护。

4.1.6 云防火墙和安全组、网络 ACL 的访问控制有什么区别？

云防火墙、安全组、网络 ACL 都可以实现通过 IP 地址/IP 地址组设置访问控制策略，为您的互联网边界和 VPC 边界、弹性云服务器、子网提供防护。

云防火墙和安全组、网络 ACL 的主要区别如表 4-2 所示。

表 4-2 云防火墙和安全组、网络 ACL 访问控制的主要区别

类别	云防火墙	安全组	网络 ACL

类别	云防火墙	安全组	网络 ACL
定义	云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和 VPC 边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持 AI 提升智能防御能力满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。	网络 ACL 是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。
防护场景	• 互联网边界 • VPC 边界 • SNAT 场景	弹性云服务器	子网
功能特性	• 支持五元组（即源 IP 地址、目的 IP 地址、协议、源端口、目的端口）过滤。 • 支持通过地理位置、域名、域名组、黑/白名单过滤。 • 支持入侵防御系统（IPS）、病毒防御（AV）功能。	支持三元组（即协议、端口和对端地址）过滤。	支持五元组（即源 IP 地址、目的 IP 地址、协议、源端口、目的端口）过滤。

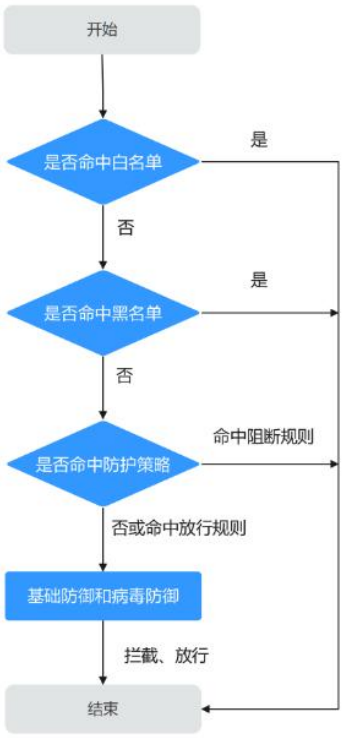
4.1.7 云防火墙支持哪些维度的访问控制？

云防火墙当前支持基于五元组、IP 地址组、服务组、域名、黑名单、白名单设置 ACL 访问控制策略；也支持基于 IPS（intrusion prevention system，入侵防御系统）设置访问控制。IPS 支持观察模式和阻断模式，当您选择阻断模式时，云防火墙根据 IPS 规则检测出符合攻击特征的流量进行阻断。

4.1.8 云防火墙的防护顺序是什么？

云防火墙匹配防护规则的优先级由高到低为：白名单 -> 黑名单 -> 防护策略（ACL）-> 基础防御（IPS）= 病毒防御（AV）。

图 4-2 防护顺序



- 设置黑/白名单请参见 3.4.4.4 管理黑白名单。
- 添加防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。
- 设置 IPS 防护模式请参见 3.5.2 配置入侵防御。
- 开启病毒防御请参见 3.5.3 配置病毒防御。

4.1.9 是否支持同时部署 WAF 和 CFW？

支持，同时部署时，流量会先经过 CFW，再经过 WAF，流量走势为：互联网 -> CFW -> WAF（独享模式）-> 源站

4.1.10 云防火墙日志默认存储多长时间？

云防火墙支持免费查询和导出 7 天内的日志记录，请参见 3.7.2 日志查询。

将单个或者多个日志记录至 LTS 中，支持查看 1~365 天的日志记录，请参见 3.7.3 日志管理。

> **⚠ 注意**
>
> LTS 按流量单独计费。

4.2 故障排查

4.2.1 流量日志和攻击日志信息不全怎么办？

CFW 只记录云防火墙开启阶段的用户流量日志和攻击日志，如果反复开启、关闭云防火墙，会导致关闭期间的日志无法记录。

因此，建议您避免反复执行开启、关闭 CFW 的操作。

4.2.2 防护规则没有生效怎么办？

配置了仅放行几条 EIP 的规则，为什么所有流量都能通过？

云防火墙开启 EIP 防护后，访问控制策略默认状态为放行。如您希望仅放行几条 EIP，您需配置阻断全部流量的防护规则，并设为优先级最低，可按如下步骤进行：

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面，根据需要选择“互联网边界”或“VPC 边界”页签。

步骤 5 配置全局阻断规则。单击“添加”按钮，在弹出的“添加防护规则”对话框中，填写参数如下，其余参数可根据您的部署进行填写。

表 4-3 放行指定 IP

参数	示例	说明
方向	**外-内**	防护的流量的方向。
源	**IP 地址** **192.168.0.0**	网络流量的发起方。
目的	**Any**	网络流量的接收方。
服务	**Any**	网络流量的协议、源端口、目的端口。
应用	**Any**	针对应用层协议的防护策略。
动作	**放行**	流量经过防火墙时的处理动作。

说明

建议您添加完所有规则后再开启“启用状态”。

步骤 6 配置放行规则。添加防护规则请参见《云防火墙用户指南》中《添加防护规则》。

步骤 7 将步骤 5 中全局阻断规则的“优先级”置为最低，具体操作请参见《云防火墙用户指南》中《设置优先级》。

步骤 8 启用所有规则。建议先开启“放行”规则，后开启“阻断”规则。

----结束

配置了全局阻断，为什么没有放行的 IP 还是能通过？

云防火墙防护 EIP 时设置的防护策略是根据“弹性公网 IP 管理列表”执行的，如果您已开启全局（0.0.0.0/0）阻断，但仍有未配置“放行”策略的 EIP 通过，需检查该 IP 是否开启防护，具体操作请参见《云防火墙用户指南》中“开启弹性公网 IP 防护”章节。

4.2.3 为什么访问控制日志页面数据为空？

问题描述

有流量产生但是访问控制日志界面没有数据。

问题原因

访问控制日志展示的是 ACL 防护策略（防护规则或黑/白名单）匹配到的流量，未开启防火墙对云资源的防护或未配置 ACL 策略都会导致访问控制日志无数据。

解决方法

1. 开启防火墙对云资源的防护：
   - 开启 EIP 防护请参见《云防火墙用户指南》中“开启弹性公网 IP 防护”章节。
   - 开启 VPC 边界防护请参见《云防火墙用户指南》中“开启 VPC 边界流量防护”章节。
2. 添加 ACL 防护策略：
   - 添加防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。
   - 添加黑/白名单请参见 3.4.4.4 管理黑白名单

相关文档

查看其它日志：

- 通过云防火墙的所有流量记录请查看流量日志。
- 攻击事件记录请查看攻击事件日志。

4.2.4 配置 CFW 防护策略后，业务无法访问怎么办？

问题描述

当您在 CFW 上配置防护策略后，业务流量出现异常，例如：

- EIP 无法访问公网
- 无法访问某个服务器
- 无法访问指定域名

排查思路

图 4-3 业务流量异常排查思路

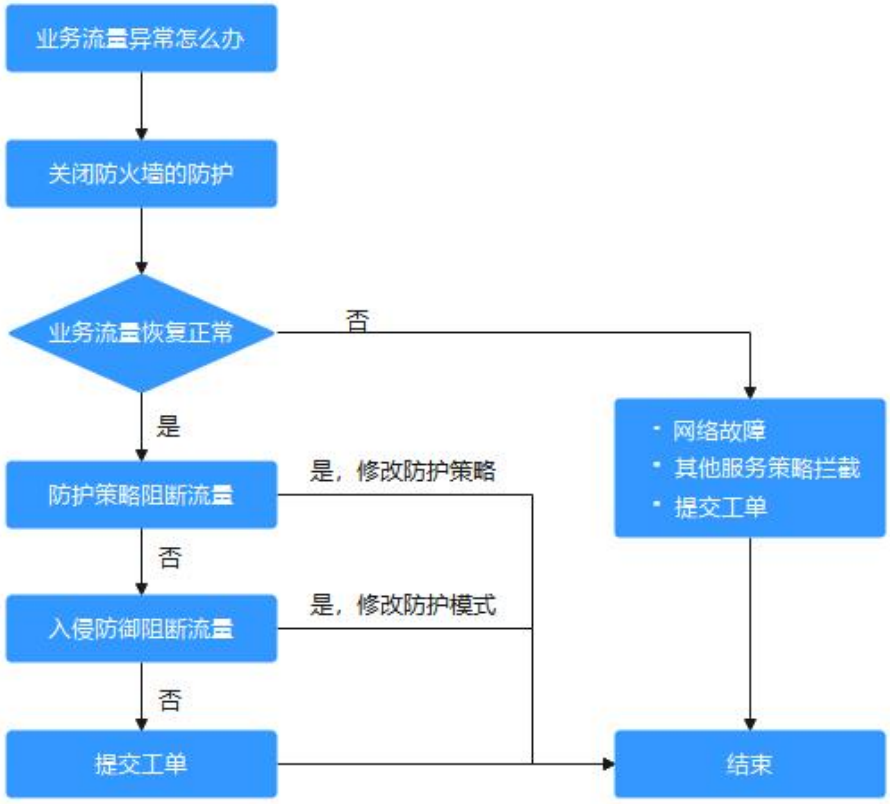


表 4-4 业务流量异常排查思路

序号	可能原因	处理措施
1	非 CFW 造成的流量中断	解决方法请参考原因一：非 CFW 造成的流量中断

序号	可能原因	处理措施
2	防护策略阻断流量	解决方法请参考原因二：防护策略阻断流量
3	入侵防御阻断流量	解决方法请参考原因三：入侵防御阻断流量

原因一：非 CFW 造成的流量中断

登录云防火墙控制台，执行以下步骤：

步骤 1 关闭防护。

- EIP 流量故障：关闭 CFW 对业务中断的 EIP 的防护，请参见关闭 EIP 防护。
- SNAT 或 VPC 间访问不通：关闭 VPC 边界防火墙的防护，请参见 3.3.2.2.3 开启/关闭 VPC 边界防火墙并确认流量经过云防火墙。

步骤 2 观察业务情况。

- 如果业务恢复，说明是 CFW 拦截了业务流量，请参见原因二：防护策略阻断流量和原因三：入侵防御阻断流量排查故障。
- 如果业务未恢复，说明非 CFW 造成的流量中断，可参考常见的故障原因：
  - 网络故障：路由配置错误，网元故障。
  - 策略拦截：其它安全服务、网络 ACL 或安全组配置错误导致的误拦截。

----结束

原因二：防护策略阻断流量

可能是在访问控制策略中配置了阻断规则，或将正常的业务加入了黑名单，此时 CFW 会阻断相关会话，导致业务受损。

您可以采取以下措施：

在访问控制日志中，搜索被阻断 IP/域名的日志记录

- 如果无记录，请参见表 4-4 原因三。
- 如果有记录，单击“规则”列跳转至匹配到的阻断策略。
  - 阻断的是黑名单，您可以选择任一方式执行：
    - 方式一：删除该条黑名单策略。
    - 方式二：增加一条该 IP/域名的白名单策略（白名单优先黑名单匹配，增加后黑名单策略失效，该流量将直接放行）。
  - 阻断的是防护规则，您可以选择任一方式执行：
    - 方式一：在访问控制规则列表中搜索相关 IP/域名的阻断策略，将阻断该 IP/域名策略停用。
    - 方式二：修改对应的阻断策略的匹配条件，移除该 IP/域名信息。

- 方式三：添加一条“动作”为“放行”用于放通该 IP/域名的防护规则，优先级高于其它“阻断”规则，添加防护规则请参见 3.4.2.1 通过防护规则拦截/放行流量。

案例

处理流程：发现故障 -> 关闭防护 -> 查看日志 -> 修改策略 -> 恢复防护 -> 确认日志

某公司的网络运维人员发现一台云服务器无法通过绑定的 EIP：xx.xx.xx.126 访问公网。

防火墙管理员做了以下措施：

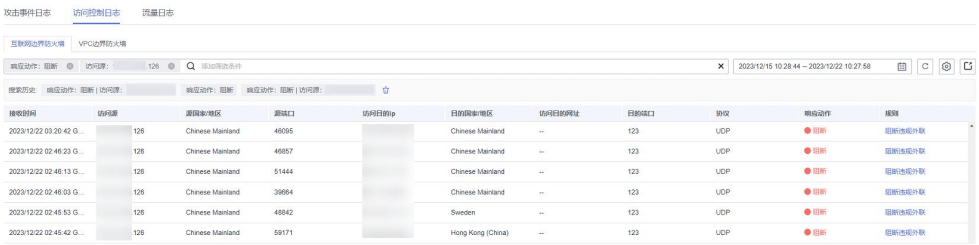
步骤 1 为优先保证问题定位期间该 IP 可以正常外联，防火墙管理员登录防火墙控制台，进入“资产管理 > 弹性公网 IP 管理”，关闭了该 EIP 的防护。

防火墙在关闭期间不再处理该 EIP 的流量，不展示相关日志。

图 4-4 弹性公网 IP 列表

步骤 2 在“日志审计 > 日志查询”的“访问控制日志”页签中筛选出了“访问源”IP 为 xx.xx.xx.126 的阻断日志，发现一条规则名为“阻断违规外联”的阻断规则，阻断了该 IP 访问外网的流量。

图 4-5 筛选访问控制日志



步骤 3 在访问控制策略列表中搜索“源：xx.xx.xx.126，动作：阻断，方向：内-外，启用状态：启用”，发现有 3 条包含该 IP 且在生效中的策略。

其中包含了“阻断违规外联”这条策略，根据“命中次数”列，可知已有大量会话被阻断。

图 4-6 搜索防护规则

⚠ 注意

图 4-5 除了第二条防护规则配置错误以外，源 IP 包含 xx.xx.xx.126 的有效策略中，优先级最高的一条“名称”为“禁止访问”，以及最低的一条“名称”为“阻断访问海外流量”，这两条策略仍会生效，需要排查这两条策略是否有拦截正常业务的风险。

经过团队内部核对，因该 IP 有访问可疑 IP 的行为，某位管理员针对该 IP 配置了阻断的防护规则，但“目的”配置错误，误将所有外联流量都阻断了（图 4-5 中第二条防护规则）。

步骤 4 管理员将目的地址修改为了需要阻断访问的特定 IP 地址后，在防火墙控制台“资产管理 > 弹性公网 IP 管理”中重新开启了该 EIP 的防护。恢复防护后该 EIP 的流量被云防火墙转发。

步骤 5 管理员在流量日志中查看到了该 IP 相关的外联日志，确认业务已恢复。

----结束

原因三：入侵防御阻断流量

IPS 等入侵防御功能防护模式设置粒度过细，阻断了正常流量。

您可以采取以下措施：

在攻击事件日志中，搜索被阻断 IP/域名的日志记录。

- 如果无记录，请联系技术支持排查问题。
- 如果有记录，参考以下两种方式处理：
  - 可复制“规则 ID”列信息，在对应的模块（如 IPS）中将动作设为观察，具体防护模块请参见 3.5.2 配置入侵防御。
  - 将不需要防火墙防护的 IP 添加到白名单，配置白名单请参见 3.4.4.4 管理黑白名单。

案例

处理流程：发现故障 -> 修改防护状态 -> 查看日志 -> 确认业务 -> 修改策略 -> 恢复防护状态 -> 确认日志

某公司的运维人员发现无法访问 IP 地址为 xx.xx.xx.99 的服务器的某种业务，疑似是由于防火墙拦截造成。

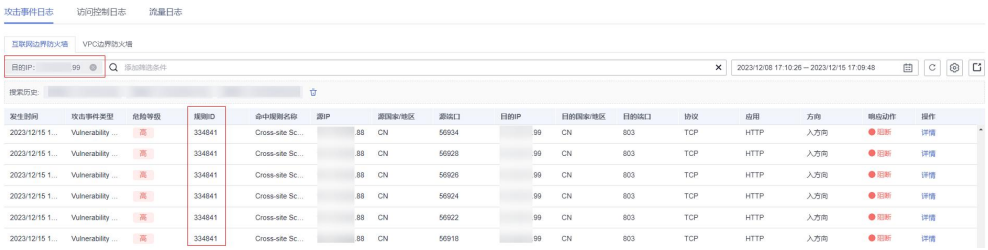
防火墙管理员做了以下措施：

步骤 1 为优先保证业务恢复，防火墙管理员登录防火墙控制台，进入“攻击防御 > 入侵防御”，将“防护模式”由“严格模式-拦截”改为“观察模式”。

在此期间，防火墙不再拦截攻击流量，只记录到攻击日志。

步骤 2 在“日志审计 > 日志查询”的“攻击事件日志”中筛选出了访问目的 IP 为 xx.xx.xx.99 的日志，发现“规则 ID”为“334841”的 IPS 规则，阻断了该流量。

图 4-7 筛选攻击事件日志



步骤 3 通过查看“详情 > 攻击 payload”，确认该业务为正常业务。于是管理员参考了 3.5.5.1 修改入侵防御规则的防护动作，在“基础防御”页签的列表中筛选出了“规则 ID”为“334841”的规则。

图 4-8 筛选“334841”的规则

步骤 4 将“操作”设置为“观察”，该 IPS 规则将不再拦截匹配到特征的流量，只做日志记录。

步骤 5 完成规则设置后，管理员将“防护模式”调回了“严格模式-拦截”，并在“基础防御”页签中确认“规则 ID”为“334841”的规则，“当前动作”仍为“观察”。

步骤 6 管理员在攻击事件日志中确认，业务会话命中该规则后，“响应动作”为“放行”，确认业务已恢复。

----结束

4.2.5 IPS 拦截了正常业务如何处理？

入侵防御（IPS）功能结合多年攻防积累的经验规则，实时检测和防护访问流量，拦截多种常见的网络攻击，有效保护您的资产。

如果已经在“攻击事件日志”中确认拦截的为正常业务流量，您可按照以下两种方式处理：

- 查询拦截该业务流量的规则 ID，并在 IPS 规则库中修改对应规则的防护动作，操作步骤请参见查询命中规则及修改防护动作。
- 降低 IPS 防护模式的拦截程度，IPS 防护模式说明请参见《云防火墙用户指南》中“配置入侵防御策略”。

查询命中规则及修改防护动作

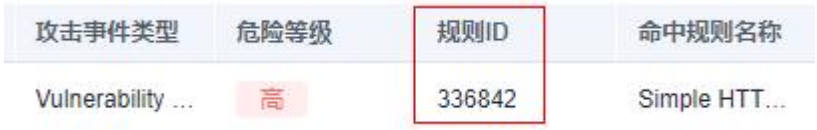
步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在左侧导航树中，选择“日志审计 > 日志查询”。进入“攻击事件日志”页面，记录拦截该业务流量的“规则 ID”。

图 4-9 规则 ID



步骤 5 单击“基础防御”栏中的“查看生效中的规则”，进入基础防御规则页面。

步骤 6 在搜索框中输入“规则 ID”搜索，并在“操作”修改为“观察”或“禁用”。

- 观察：修改为“观察”状态，修改后防火墙对匹配当前防御规则的流量，记录至日志中，不做拦截。
- 禁用：修改为“禁用”状态，修改后防火墙对匹配当前防御规则的流量，不记录、不拦截。

----结束

相关文档

业务无法正常访问，但不是 IPS 拦截，处理方式请参见 4.2.4 配置 CFW 防护策略后，业务无法访问怎么办？。

4.2.6 配置 LTS 日志时提示权限不足怎么办？

在“日志管理”页面，完成日志配置后，提示“您的权限不足”，此时需要添加“LTS FullAccess”权限。

问题描述

“日志管理”页面，提示“您的权限不足”。

问题原因

“日志管理”页面，是将日志转储到云日志服务（Log Tank Service，简称 LTS）中，此页面的所有操作，需要调用 LTS 服务的接口，依赖 LTS 服务权限。

解决方法

由主账号给子账号添加“LTS FullAccess”权限，授权操作请参见《云日志服务用户指南》中“授权 IAM 用户使用云日志服务 LTS”章节。

4.2.7 开启了 EIP 自动防护但不生效怎么办？

问题描述

在“资产管理 > 弹性公网 IP 管理”页面，开启了“新增 EIP 自动防护”，但新购买的 EIP 未被 CFW 防护，即“防护状态”是“未防护”。

问题原因

“新增 EIP 自动防护”开启后，CFW 会在整点自动同步 EIP 资源至列表中，同步后才会对新增的 EIP 开启防护。

解决方法

您可以等待 CFW 自动开启防护或者手动开启 EIP 防护，手动开启防护操作请参见 3.3.1 开启互联网边界流量防护。

4.3 网络流量

4.3.1 VPC 个数和 VPC 边界防护流量峰值如何计算？

专业版云防火墙默认防护 2 个 VPC，提供 200Mbps 的 VPC 边界流量防护，如果您需要防护更大的 VPC 间流量，可以通过购买 VPC 数量扩展，每个 VPC 支持 200M 的 VPC 边界流量防护。

例如：业务部署需要防护 1Gbps 的 VPC 边界流量，则云防火墙默认防护 2 个 VPC（200M），您还需购买 4 个 VPC（4*200M），VPC 边界防护流量=默认值（200M） + 4*VPC（200M）= 1Gbps。

4.3.2 云防火墙数据流量怎么统计？

云防火墙流量统计分为两种形式：

- 基于流量统计数据。
  在“总览”页面的“流量趋势”模块中查看；数据信息实时更新。
- 基于会话统计数据，流量在会话结束的瞬间时刻统计。

- 在“日志审计 > 日志查询 > 流量日志”页面查看；数据信息是会话创建到结束期间的整体流量；在会话连接期间，数据不会上报，连接结束后才会上报。
- 在“流量分析”下的任意页面查看；数据信息是流量日志中在该时间结束会话的流字节数的平均值。

4.3.3 云防火墙提供的防护带宽是多少？

云防火墙为您提供互联网边界和 VPC 之间的防护，您可根据需要扩展防护带宽。根据您购买的服务版本的不同，云防火墙提供不同规格的防护带宽：

- 互联网方向：标准版默认 10Mbps，专业版默认 50Mbps。
- VPC 间防护：标准版不提供基础防护流量，专业版默认 200Mbps。

4.3.4 业务流量超过防护带宽怎么办？

如果您的实际业务流量超过防护带宽流量，可能出现限流、随机丢包、自动 Bypass 等现象，导致您的部分业务在一定时间内不可用、卡顿、延迟等。

如果出现这种情况，您需要及时根据实际业务情况购买扩展包来提供足够的防护带宽。如果您的业务流量浮动较大，建议参考“总览”页面中的“运营看板”模块，根据“出方向 95 带宽”或“入方向 95 带宽”的最大值购买。

说明

- 云防火墙支持设置流量超额预警，当业务流量达到已购买带宽规格的一定比例时，将发送告警通知，设置告警通知请参见 3.8.1 告警通知。
- 95 带宽：系统每个周期统计 1 个带宽值，将某段时间内的带宽值进行降序排列，去掉带宽数值最高的前 5%的值，剩余的最高带宽即为 95 带宽。

  例如：出方向 95 带宽为 100bps，则在某段时间（例如 24 小时）内，带宽值经过降序排列并去掉最高的 5%的值后，剩余的最高带宽为 100bps。

4.3.5 流量趋势模块和流量分析页面展示的流量有什么区别？

两个模块流量数据的统计方式不同：

- “总览”页面的“流量趋势”模块基于流量统计数据，数据信息实时更新；展示的内容为入方向流量、出方向流量、VPC 间流量信息。
- “流量分析”页面基于会话统计数据，在会话连接期间，数据不会上报，连接结束后才会上报。
  - 入云流量：入云方向的会话。
  - 出云流量：出云方向的会话。
  - VPC 间访问：VPC 间的会话。

4.3.6 如何验证 HTTP/HTTPS 的出方向域名防护规则的有效性？

可按照以下操作步骤验证有效性：

步骤 1 发送 HTTP 或 HTTPS 请求。

- 方式一：使用 curl 命令，例如：

```
curl -k "https://www.example.com"
```

- 方式二：使用浏览器访问域名。

⚠ 注意

请勿使用 telnet 命令进行域名测试。

使用 telnet 命令对域名和端口进行测试时（例如 telnet www.example.com 80），只会生成 TCP 握手流量，并不会模拟完整的 HTTP 或 HTTPS 请求，此时应用类型识别为 Unknown，不会被 HTTP 或 HTTPS 应用策略命中。

步骤 2 进入管理控制台，查看防护规则的命中次数和日志记录，如果有新增，说明规则生效，如果无新增，请及时修改防护规则。

1. 在“访问控制 > 访问策略管理”的“防护规则”页签中，查看规则的“命中次数”。
2. 在“日志审计 > 日志查询”的“访问控制日志”页签中，查看该规则的防护记录。

----结束

4.3.7 如何获取攻击者的真实 IP 地址？

流量经过反向代理后，源 IP 被转换为回源 IP，此时如果受到外部攻击，CFW 无法通过源 IP 获取到攻击者的真实 IP 地址，您可通过攻击事件日志中的 X-Forwarded-For 字段查询真实 IP 地址。

查看 X-Forwarded-For

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

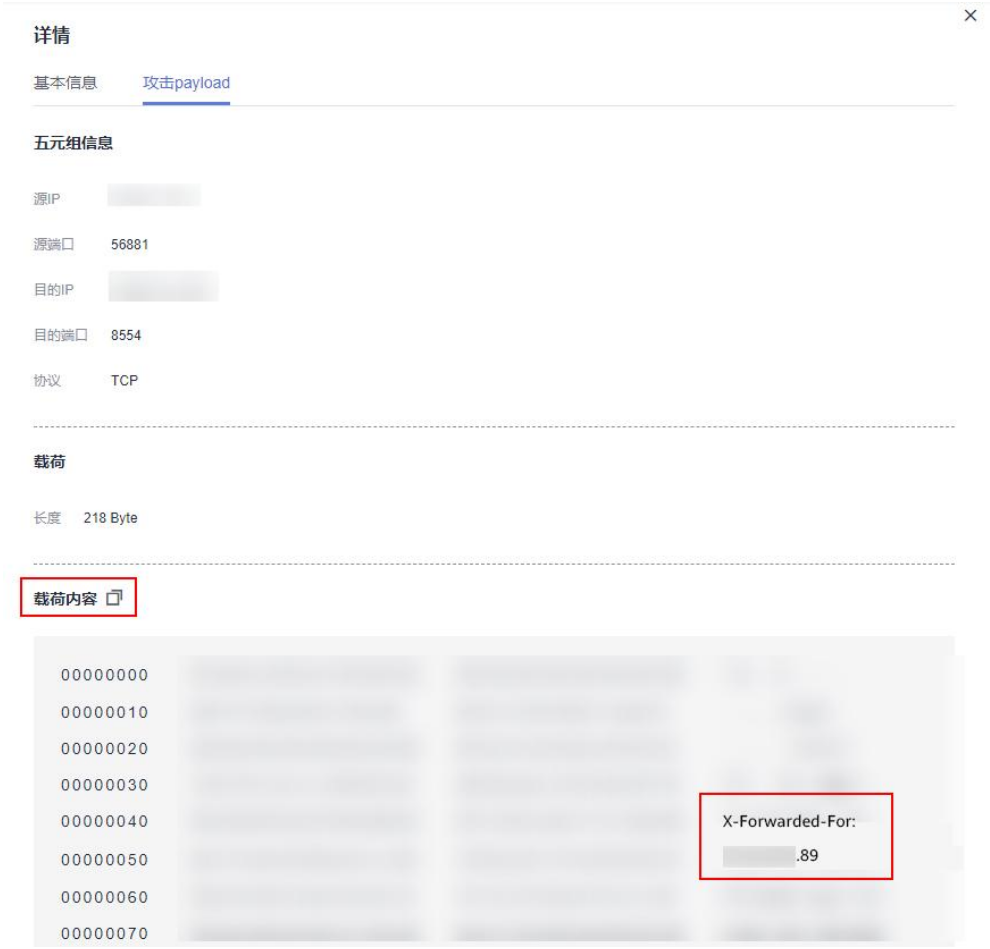
步骤 4 在左侧导航树中，选择“日志审计 > 日志查询”。进入“攻击事件日志”页面，在对应事件的“操作”列，单击“详情”。

图 4-10 查看攻击事件日志详情

步骤 5 在“详情”中，切换至“攻击 payload”页签，获取 X-Forwarded-For 字段。

- 方法一：在“载荷内容”中查看 X-Forwarded-For（从客户端到最后一个代理服务器的所有地址 IP）。

图 4-11 载荷内容中 X-Forwarded-For



- 方法二：复制“载荷内容”，通过 Base64 工具，获得解码结果：
  - X-Forwarded-For：从客户端到最后一个代理服务器的所有地址 IP

  例如，通过图 4-11 可得真实客户端的 IP 为 xx.xx.xx.89，只经过云模式 WAF 的一层代理。

图 4-12 Base64 解码结果示例

----结束

4.4 计费类

4.4.1 云防火墙如何收费和计费？

云防火墙支持包年/包月（预付费）和按需计费（后付费）两种计费方式。

其中标准版支持扩容防护公网 IP 数和互联网边界流量峰值。

专业版支持扩容防护公网 IP 数、互联网边界流量峰值和防护 VPC 数。

4.4.2 云防火墙如何变更版本规格？

云防火墙，支持标准版升级到专业版，不支持专业版变更到标准版。如需降低版本规格，需退订当前版本后再进行购买。

有关退订 CFW 的详细操作，请参见 4.4.4 如何退订云防火墙？。

从标准版升级到专业版

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤 4 在页面左上角，单击“升级到专业版”，进入升级云防火墙页面。

步骤 5 确认版本规格后，单击“立即购买”。

----结束

4.4.3 如何为云防火墙续费？

该任务指导用户如何在云防火墙即将到期时进行续费。续费后，用户可以继续使用云防火墙。

- 购买的服务版本到期前，系统会以短信或邮件的形式提醒您服务即将到期，并提醒您续费。
- 购买的服务版本到期后，如果没有按时续费，公有云平台提供一定的保留期。

说明

为了防止造成不必要的损失，请您及时续费。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航栏中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的总览页面。

步骤 3 在界面“防火墙详情”模块的右上角，单击“续费”。

步骤 4 选择云防火墙的续费时长，判断是否勾选“统一到期日”，将云防火墙到期时间统一到各个月的某一天。

步骤 5 确认配置费用后单击“去支付”。

步骤 6 进入支付页面，选择支付方式，确认付款，支付订单后即可完成续费。

----结束

4.4.4 如何退订云防火墙？

退订后原 CFW 配置数据将不能保存且无法找回，建议您退订前导出防护策略，重购后导入防护策略，以便 CFW 更好的为您防护。有关导入导出策略的详细操作，请参见 3.4.4.1 导入/导出防护策略。

操作步骤

请参见《费用中心》中《退订流程》章节。

A 修订记录

发布日期	修改说明
2025-07-24	第八次正式发布。 新增： 3.10 使用 CTS 审计 CFW 操作事件章节。
2025-05-07	第七次正式发布。 新增： • 1.3 产品功能章节，合入“功能特性”和“服务版本差异”章节内容。 • 4.1.2 云防火墙支持防护哪些范围？章节。 • 4.2.7 开启了 EIP 自动防护但不生效怎么办？章节。 • 4.2.6 配置 LTS 日志时提示权限不足怎么办？章节。 • 4.3.2 云防火墙数据流量怎么统计？章节。 • 4.1.3 云防火墙支持的 QPS、新建/并发连接数大小是多少？章节。 优化： • 3.4.1 访问控制策略概述，增加防护策略的应用场景和特点。 • 3.4.5.1 管理 IP 地址组章节，添加、删除等操作合并。 • 3.4.5.2 管理域名组章节，添加、删除等操作合并。 • 3.4.5.3 管理服务组章节，添加、删除等操作合并。
2024-12-17	第六次正式发布。 新增： • 3.1.2 升级云防火墙版本章节。 • 3.1.3 变更云防火墙扩展包数量章节。 • 4.4.2 云防火墙如何变更版本规格？章节。

发布日期	修改说明
2024-07-11	第五次正式发布。 新增： • 1.7 术语解释章节中，防护流量概念。 • 3.3.3 开启 NAT 网关流量防护章节。 • 3.4.1 访问控制策略概述章节。 • 3.4.2.1 通过防护规则拦截/放行流量章节中，NAT 流量防护规则。 • 3.4.3 通过策略助手查看防护信息章节。 • 3.9.5.1.2-查看预定义地址组章节。 • 3.9.5.3.2-查看预定义服务组章节。 • 3.5.3 配置病毒防御章节。 • 3.5.4 通过安全看板查看攻击防御信息章节。 • 3.15.6-失败配置处理章节。 • 3.7.2 日志查询章节中，相关操作和后续操作。 • 3.7.3 日志管理章节。 • 3.8.3 安全报告管理章节。 • 4.1.6 云防火墙和安全组、网络 ACL 的访问控制有什么区别？章节。 • 4.1.8 云防火墙的防护顺序是什么？章节。 • 4.1.9 是否支持同时部署 WAF 和 CFW？章节。 • 4.1.10 云防火墙日志默认存储多长时间？章节。 • 4.2.4 配置 CFW 防护策略后，业务无法访问怎么办？章节。 • 4.2.5 IPS 拦截了正常业务如何处理？章节。 • 4.2.3 为什么访问控制日志页面数据为空？章节。 • 4.3.5 流量趋势模块和流量分析页面展示的流量有什么区别？章节。 • 4.3.7 如何获取攻击者的真实 IP 地址？章节。 优化： • 1.4 使用限制章节。 • 3.2 云防火墙防护总览章节。 • 3.6 流量分析章节。 章节名称优化： • “ 云防火墙控制台概览”更名为“查看概览”。 • “开启弹性公网 IP 防护”更名为“开启互联网边界流量防护”。 • “管理 VPC 边界防火墙”更名为“开启 VPC 边界流量防护”。 • “配置企业路由器”更名为“配置企业路由器将流量引至云防火墙”。
2025-07-24	• “管理访问控制策略”更名为“管控 EIP/VPC 访问流量”。 • “添加防护规则”更名为“通过配置防护规则拦截/放行流量”

发布日期	修改说明
2023-11-28	第四次正式发布。 新增： • 3.2 云防火墙防护总览章节中，流量态势和流量趋势。 • 3.4.3 通过策略助手查看防护信息章节。 • 3.5.3 配置病毒防御章节。 • 3.5.4 通过安全看板查看攻击防御信息章节。 • 3.6 流量分析及子章节。 • 3.8.1 告警通知章节中，EIP 未防护告警。 • API 类及子章节。 优化： • 1.4-功能特性章节中，流量分析内容。 • 1.3 产品功能章节中，版本差异内容。 • 3.1.1 购买云防火墙章节中，引擎名称。 • 3.3.2 开启 VPC 边界流量防护及子章节。 • 3.7.2 日志查询章节中，新增地理位置参数。

发布日期	修改说明
2023-10-10	第三次正式发布。 新增： • 3.2 云防火墙防护总览章节中，“安全概览”和“流量趋势”功能。 • 1.4 使用限制。 • 与企业路由器的关系。 • 查看弹性公网 IP 信息。 • 3.3.2 开启 VPC 边界流量防护及其子章节。 • 3.4.2.1 通过防护规则拦截/放行流量章节中“配置示例”。 • 3.4.5.2 管理域名组。 • 3.5.2 配置入侵防御章节中，“敏感目录扫描防御”和“反弹 Shell 检测防御”功能。 • 3.5.5 IPS 规则管理。 • 3.5.5.2 自定义 IPS 特征。 • 3.9 使用 CES 监控 CFW 及其子章节。 • 4.1.6 云防火墙和安全组、网络 ACL 的访问控制有什么区别？。 • 4.1.8 云防火墙的防护顺序是什么？。 • 4.3.1 VPC 个数和 VPC 边界防护流量峰值如何计算？。 • 4.2.5 IPS 拦截了正常业务如何处理？。 • 4.4.2 云防火墙如何变更版本规格？。 优化： • 查看访问控制规则列表、3.4.4.3 管理防护规则、复制防护规则（合入管理防护规则）、删除防护规则（合入管理防护规则）章节合入 3.4.4 管理访问控制策略。 • 3.4.4.4 管理黑白名单、3.4.5.3 管理服务组章节合入 3.4 访问控制。 • 3.8.2 DNS 服务器配置章节更换至 3.8 系统管理，并更新入口信息。 删除： “关闭弹性公网 IP 防护”章节。
2023-05-23	第二次正式发布。 新增： • 1.4 使用限制。 • 1.7 术语解释。 • 2 计费说明。 • 4.4 计费类。

发布日期	修改说明
2023-03-07	第一次正式发布。