天翼云·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 5
1.1 产品定义及优势 5
1.2 功能特性 6
1.3 应用场景 7
1.4 使用限制 7
1.5 术语解释 7
1.6 等保合规能力说明 9
1.7 用户权限 11
1.8 与其它云服务的关系 12
2 计费说明 13
3 用户指南 15
3.1 购买云防火墙 15
3.2 云防火墙控制台概览 16
3.3 管理弹性公网 IP 防护 17
3.3.1 开启弹性公网 IP 防护 17
3.3.2 关闭弹性公网 IP 防护 19
3.4 管理访问控制策略 20
3.4.1 添加防护规则 20
3.4.2 批量管理防护规则 23
3.4.3 查看访问控制规则列表 26
3.4.4 编辑防护规则 27
3.4.5 设置优先级 27
3.4.6 删除防护规则 28
3.4.7 管理黑/白名单 28
3.4.7.1 添加黑/白名单 28
3.4.7.2 编辑黑/白名单 29
3.4.7.3 删除黑/白名单 30
3.4.8 配置 DNS 解析 31
3.5 管理 IP 地址组 32
3.5.1 添加 IP 地址组 32

3.5.2 添加 IP 地址 32
3.5.3 删除 IP 地址组 33
3.6 管理服务组 34
3.6.1 添加服务组 34
3.6.2 添加服务 34
3.6.3 删除服务组 35
3.7 配置入侵防御策略 36
3.8 管理基础防御规则 37
3.8.1 查看 IPS 规则库 37
3.8.2 修改基础防御规则动作 39
3.9 流量分析 40
3.10 日志审计 41
3.10.1 日志查询 41
3.11 系统管理 44
3.11.1 告警通知 44
4 常见问题 47
4.1 产品咨询类 47
4.1.1 云防火墙支持线下服务器吗？ 47
4.1.2 云防火墙支持跨帐号使用吗？ 47
4.1.3 云防火墙与 Web 应用防火墙有什么区别？ 47
4.1.4 QPS 高，流量峰值就高吗？ 48
4.2 功能类 48
4.2.1 通过日志审计功能可查看哪些信息？ 48
4.2.2 云防火墙支持哪些维度的访问控制？ 48
4.2.3 云防火墙攻击日志，为什么显示还未纳入防护的 EIP？ 48
4.3 故障排查类 48
4.3.1 流量分析页面发现流量日志和攻击日志不全怎么办？ 48
4.3.2 配置了策略为什么没有生效？ 49
4.3.3 Apache Log4j 远程代码执行漏洞攻击，云防火墙如何启用检测和防御？ 49
4.3.4 Spring Framework 远程代码执行漏洞攻击，云防火墙如何启用检测和防御？ 50
4.4 网络流量类 51
4.4.1 流量分析功能有哪些？ 51
4.4.2 云防火墙数据流量怎么统计？ 51
4.4.3 单条流量超速，需要升级带宽吗？ 51
4.4.4 云防火墙提供的防护带宽流量是多少？ 51
4.5 计费类 52
4.5.1 云防火墙如何收费和计费？ 52
4.5.2 如何为云防火墙续费？ 52
4.5.3 如何退订云防火墙？ 52

A 修订记录 53

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，同时支持按需弹性扩容、AI 提升智能防御能力、灵活扩展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。

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、暴力破解等攻击。

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及跨 ECS 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；同时，带宽/EIP/安全策略等关键性能规格可无限扩展，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。具体配置步骤请参见《云防火墙用户指南 > 管理访问控制策略》。

- 支持对 IP 地址组、 黑名单、白名单设置 ACL 访问控制策略。

1.2 功能特性

云防火墙提供了“云防火墙标准版”供您使用，包括访问控制、入侵防御、流量分析以及日志审计等功能。

表1-1 功能特性

功能项	功能描述
概览	提供已开启和未开启的防火墙状态总览。
资产管理	查看和管理弹性公网 IP 的相关数据及信息。
访问控制	支持互联网边界流量的访问控制。
入侵防御	提供对互联网流量的入侵检测与防护，可选择防护模式及是否开启基础防御。 基础防御包括威胁检测及漏洞扫描，主要检测以下两点： • 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。 • 检测是否存在协议异常、缓冲区溢出、访问控制、可疑 DNS 活动及其他可疑行为。
流量分析	为您展示互联网业务访问流量统计数据和已检测出的入侵攻击风险统计数据。 • 互联网出入口流量统计：展示最近 1 小时、最近 24 小时、最近 7 天的数据。 • 入侵攻击事件统计：展示最近 1 小时、最近 24 小时、最近 7 天的数据。
日志审计	支持入侵攻击事件日志、访问控制日志、流量日志。其中： • 攻击事件日志：入侵攻击事件的详细信息。 • 访问控制日志：可以查看哪些访问放行，哪些访问被阻断的详细信息。 • 流量日志：可以查看具体某个业务的访问流量信息。
系统管理	告警通知：用户可以通过云防火墙服务对攻击日志和流量超额预警进行通知设置。开启告警通知后，CFW 可将 IPS 攻击日志和流量超额的预警信息通过用户设置的接收通知方式（例如邮件或短信）发送给用户。

表1-2 直路引擎

名称	主要功能描述	支持协议	支持场景
直路引擎	用户流量先经过防火墙直路引擎，进行安全检测与防护后，再将流量送至目标 ECS。检测功能丰富，阻断策略灵活。	TCP、UDP、ICMP、Any、ICMPV6	可以支持互联网边界的防护。

1.3 应用场景

外部入侵防御

通过云防火墙，对已开放公网访问的服务资产进行安全盘点，可一键开启入侵检测与防御。

主动外联管控

云防火墙支持基于域名的访问控制，可对主动外联行为进行精准管控。

等保合规

云防火墙可满足《网络安全等级保护 2.0》中对区域边界防护、网络入侵防范、网络访问控制、安全日志审计等检查要求。

1.4 使用限制

- CFW ALG 标签功能受限。
- CFW 默认不开启网络层流量类型 DDoS 攻击与 IP 欺骗防御功能。
- 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，建议优先使用自定义域名服务器。
- 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、扩容引擎）需要客户端重新发起连接。

1.5 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。

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 可以绑定到用户帐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帐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他地方之前阻止该恶意通信。

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，重要网络区域与其他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。	《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断、开通或变更白名单策略。	《功能特性》
		应能够对非授权设备私自联到内部网络的行为进行限制或检查。	中		
		应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	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	中	云防火墙提供对业务流量中的攻击行为的检测	

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
		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。		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》
		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。	

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》
		审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	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 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。若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。

1.8 与其它云服务的关系

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 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 Web 服务提供防护。

WAF 和 CFW 的主要区别说明如表 1-3 所示。

表1-3 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，同时支持按需弹性扩容、AI 提升智能防御能力、灵活扩展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。 • 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：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。

2 计费说明

计费项

CFW 根据您的 CFW 服务版本、购买时长和购买的计费项目计费。

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。

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 购买云防火墙

云防火墙支持一个帐号下购买多个防火墙，便于管理不同场景下的资源和策略。

云防火墙支持包年/包月（预付费）计费方式。同时，包周期（包年/包月）提供以下服务版本：标准版。您可以根据业务需求购买云防火墙。

前提条件

当前帐号拥有 BSS Administrator 权限。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

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 购买云防火墙的参数说明

参数名称	参数说明	取值样例
区域	购买互联网边界防火墙的区域。	广东-广州
版本规格	选择版本： • 标准版	标准版
引擎类型	选择引擎类型： • 山石引擎：直路部署。具备精细化应用管控，可为用户提供灵活的安全访问控制，包括策略阻止、会话限制等。同时，还具备入侵防御、病毒过滤、攻击防护等功能，满足客户安全访问、攻击防护以及应用识别和控制等需求。	直路引擎

参数名称	参数说明	取值样例
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 说明 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。	45 个
扩展防护流量峰值	（可选）选择需扩展的防护流量峰值，可选择范围：0~2000Mbps/月（需为 5 的整数倍） 说明 • 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/月（套餐内费用包含），如果您的防护流量是 200Mbps/月，那么只需要填写 190Mbps/月。 • 扩展防护流量峰值是所有 eip 防护带宽叠加的峰值。	200Mbps/月
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。	CFW
高级设置	标签：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。	1 年

步骤 4 确认购买信息无误后，单击“立即购买”。

----结束

3.2 云防火墙控制台概览

概览页面向您展示云防火墙的服务介绍、版本状态及防护统计信息。包括：引擎类型、弹性公网 IP 的总数量及防护数量、可防护流量峰值、日志存储空间等信息。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 查看云防火墙的运行状态、引擎类型、防护状态等信息。

表3-2 防火墙详情页面参数说明

参数名称	参数说明
EIP 总数量	开启防护及关闭防护的弹性公网 IP 总数量。
防护数量	开启防护的弹性公网 IP 数量。
未防护数量	关闭防护的弹性公网 IP 数量。
覆盖率	开启防护的弹性公网 IP 数量占弹性公网 IP 总数量的百分比。
状态	云防火墙的状态。开通或退订防火墙大约需要 5 分钟更新状态。
引擎类型	当前防火墙的引擎类型： • 山石引擎：直路部署。具备精细化应用管控，可为用户提供灵活的安全访问控制，包括策略阻止、会话限制等。同时，还具备入侵防御、病毒过滤、攻击防护等功能，满足客户安全访问、攻击防护以及应用识别和控制等需求。
已使用/可防护 EIP 数	已开启防护的弹性公网 IP 数量。
可防护流量峰值	可防护的南北向流量峰值。
计费模式	购买的计费模式。

----结束

3.3 管理弹性公网 IP 防护

3.3.1 开启弹性公网 IP 防护

未开启弹性公网 IP 防护时，您的业务流量不会经过云防火墙。

开启防护后，您需配置访问控制策略或开启 IPS 开关，云防火墙才会实施拦截操作，配置访问控制策略请参见 3.4.1 添加防护规则，IPS 相关请参见 3.7 配置入侵防御策略。

本文指导您同步 EIP 信息并开启弹性公网 IP 防护，如您想对某 IP 关闭防护，请参见 3.3.2 关闭弹性公网 IP 防护。

约束条件

弹性公网 IP 防护目前不支持 IPv6。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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。

单击页面右上角“资产同步”，将您的弹性公网 IP 信息导入至列表中，刷新弹性公网 IP 列表。

须知

- 弹性公网 IP 防护目前不支持 IPv6。
- 当前帐号下有多个云防火墙时，资产同步只将“未防护”的 EIP 同步至列表中。

步骤 4 （可选）当您列表 IP 数量过多时，可执行此步骤进行筛选。

在页面上方搜索下拉框中，选择搜索类型并输入信息，回车键确认，可添加多个筛选条件，右侧 🔍 进行搜索。

- 弹性公网 IP 地址/ID：根据 IP 地址搜索，即“弹性公网 IP”列；或对应的 ID 号，由系统自动生成，即“ID”列。
- 企业项目名称：根据 IP 归属的企业项目名称搜索，即“企业项目信息”列。
- 已绑实例名称/ID：根据实例名称搜索，如“云服务器”，即“已绑定实例”列中黑色字体的信息；实例名称的 ID 号，如“ecs-ndr-0909”，即“已绑定实例”列中蓝色字体的信息。
- 弹性 IP 标签：根据弹性公网 IP 设置标签分类搜索。
- 防火墙名称/ID：根据防火墙名称或 ID 搜索，即“防火墙名称/ID”列。

说明

- 搜索类型支持模糊搜索。
- 未选择搜索类型时，默认类型为弹性公网 IP 地址/ID。

步骤 5 开启弹性公网 IP。

- 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，单击表格上方的“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”。

说明

EIP 开启防护后，访问控制策略默认动作为“放行”。

----结束

后续操作

- 配置防护规则：3.4.1 添加防护规则。
- 开启基础防御：3.7 配置入侵防御策略。

3.3.2 关闭弹性公网 IP 防护

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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。

步骤 4 （可选）当您列表 IP 数量过多时，可执行此步骤进行筛选。

在页面上方搜索下拉框中，选择搜索类型并输入信息，回车键确认，可添加多个筛选条件，右侧 🔍 进行搜索。

- 弹性公网 IP 地址/ID：根据 IP 地址搜索，即“弹性公网 IP”列；或对应的 ID 号，由系统自动生成，即“ID”列。
- 企业项目名称：根据 IP 归属的企业项目名称搜索，即“企业项目信息”列。
- 已绑实例名称/ID：根据实例名称搜索，如“云服务器”，即“已绑定实例”列中黑色字体的信息；实例名称的 ID 号，如“ecs-ndr-0909”，即“已绑定实例”列中蓝色字体的信息。
- 弹性 IP 标签：根据弹性公网 IP 设置标签分类搜索。
- 防火墙名称/ID：根据防火墙名称或 ID 搜索，即“防火墙名称/ID”列。

说明

- 搜索类型支持模糊搜索。
- 未选择搜索类型时，默认类型为弹性公网 IP 地址/ID。

步骤 5 关闭弹性公网 IP。

- 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”。

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

----结束

3.4 管理访问控制策略

3.4.1 添加防护规则

配置合适的访问控制策略能有效的帮助您对内部服务器与外网之间的流量进行精细化管控，防止内部威胁扩散，增加安全战略纵深。

EIP 开启防护后，访问控制策略默认状态为放行，如您希望仅放行几条 EIP，建议您添加一条优先级最低的阻断全部流量的防护规则。

前提条件

已进行同步资产操作并开启弹性公网 IP 防护，请参见 3.3.1 开启弹性公网 IP 防护。

互联网边界防护规则

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 添加新的防护规则。

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

表3-3 添加防护规则-互联网边界

参数名称	参数说明	取值样例
方向	选择防护方向： • 外到内：外网访问内部服务器。 • 内到外：客户服务器访问外网。	内到外
名称	自定义规则名称。	test
源类型	选择 **IP 地址**、**IP 地址组**或**地域**。 • **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

参数名称	参数说明	取值样例
	• **IP 地址组**：支持多个 IP 地址的集合。 • **地域**：支持地域防护，可在“源地址”中选择地区。	
源地址	设置访问流量中发送数据包的参数。 “源类型”为“IP 地址”时，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 “源类型”为“IP 地址组”时，选择 IP 地址组。	192.168.10.5
目的类型	选择 **IP 地址**、**IP 地址组**。 • **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。 说明 “方向”为“内-外”时，支持选择“域名”类型。	IP 地址
目的地址	设置访问流量中的接收数据包的参数。 • “目的类型”为“IP 地址”时，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 • “目的类型”为“IP 地址组”时，选择 IP 地址组。 • “目的类型”为“域名”时，支持多级别单域名（例如，一级域名 example.com，二级域名 www.example.com 等）。 说明 • 若域名为精准域名，输入后需单击右侧“测试”，以测试域名有效性，并进行 DNS 解析，请参见《云防火墙用户指南 > 配置 DNS 解析》。	192.168.10.6
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
协议类型	协议类型当前支持：TCP、UDP、ICMP、Any。	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。 • 支持连续端口组，中间使用“-”隔开，如：80-443。	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。 • 支持连续端口组，中间使用“-”隔开，如：80-443。	443
是否支持长连接	“协议类型”选择“TCP”或“UDP”时，需要设置是否配置长连接。 • 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。 **说明** **最大支持 100 条规则设置长连接。**	是
长连接设置时长	“是否支持长连接”选择“是”时，需要配置此参数。 设置长连接时长。输入“时”、“分”、“秒”。 **说明** **支持时长设置为 1 秒~1000 天。**	60 时 60 分 60 秒
动作	选择“放行”或者“阻断”。设置相应流量是否通过云防火墙。	放行
策略优先级	设置该策略的优先级： • 置顶：表示将该策略设置为最优先级别。 • 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。 **说明** **设置后，优先级数字越小，策略的优先级越高。**	置顶
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。	
标签	用于标识规则，可通过标签实现对云资源的分类和搜索。	-

步骤 5 单击“确认”，完成配置安全策略。

说明

EIP 开启防护后，访问控制策略默认状态为放行，如您希望仅放行几条 EIP，建议您添加一条优先级最低的阻断全部流量（0.0.0.0/0）的防护规则。

----结束

3.4.2 批量管理防护规则

如果您需批量添加和导出防护规则，请参照本章节进行处理。

批量导入防护规则操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 单击“下载模板”，下载导入规则模板到本地。

步骤 5 请按表格要求填写您要添加的防护规则信息，防护规则参数说明如表 3-4 所示。

须知

- 目前最大支持导入 300 条规则，其中单个源地址组或服务组的成员不能超过 64 个。
- 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。

表3-4 防护规则参数说明

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
方向	选择防护方向： • 外到内：外网访问内部服务器。 • 内到外：客户服务器访问外网。	内到外
动作	选择“放行”或者“阻断”。设置相应流量是否通过云防火墙。	放行
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

参数名称	参数说明	取值样例
源地址类型	设置访问流量中发送数据的地址类型。 • **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	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	选择访问流量中的接收数据的地址类型。 • **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
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	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
域名	“目的地址类型”选择“域名”时，需填写“域名”。	www.example.com

参数名称	参数说明	取值样例
	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。	
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、ICMPV6。 • 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

步骤 6 表格填写完成后，单击“导入规则”按钮，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。

步骤 7 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 8 返回防护规则列表查看导入的防护规则。

----结束

批量导出防护规则操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 单击“导出规则”，导出规则到本地。

----结束

3.4.3 查看访问控制规则列表

您可通过列表查看当前设置的访问控制信息，包括源 IP 与目的 IP 拦截或放行的动作、方向、优先级等详情。

前提条件

已添加防护规则。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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。

表3-5 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。 说明 数字越小策略的优先级越高。
名称	自定义规则名称。
访问源	访问流量中发送数据包的地址参数。
目的	访问流量中接收数据包的地址参数。
协议/源端口/目的端口	• 协议类型当前支持：TCP、UDP、ICMP、Any、ICMPV6。 • 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。
启用状态	当前规则的启用状态，支持启用和禁用。
动作	• “放行”：设置相应流量通过云防火墙。 • “阻断”：阻止相应流量通过云防火墙。
IP 类型	当前规则防护的 IP 类型，支持 IPv4 和 IPv6。
方向	• 内到外：客户服务器访问外网。 • 外到内：外网访问内部服务器。

参数名称	参数说明
命中次数	当前规则已放行或阻断的次数。
描述	当前规则的备注信息。
长连接设置时长	当前规则设置的长连接时长。

步骤 4 （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，或者在“名称/IP 地址”搜索栏搜索需要查看的规则。

----结束

3.4.4 编辑防护规则

当您需修改已添加的防护规则的方向、名称、源类型等配置参数时，可以参考本章节进行修改操作。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 在需要编辑的防护规则所在行的“操作”列，单击“编辑”。

步骤 5 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 6 修改完成后，单击“确认”保存。

----结束

3.4.5 设置优先级

如您需调整放行或阻断 IP 的优先级顺序您可以参照本节步骤设置规则的优先级。

1 为最高优先级，数字越大，优先级越低。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 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 5 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 6 单击“确认”，完成设置优先级。

----结束

3.4.6 删除防护规则

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 在需要删除的防护规则所在行的“操作”列，单击“删除”。

步骤 5 在弹出的“删除规则”界面，单击“是”，完成删除。

⚠ 警告

删除规则后无法恢复，请谨慎操作。

----结束

3.4.7 管理黑/白名单

3.4.7.1 添加黑/白名单

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。

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）。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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。选择“黑名单”或“白名单”页签。

步骤 4 单击“添加黑名单”或“添加白名单”，设置地址方向、IP 地址、协议类型、端口，填写规则请参照表 3-6。

表3-6 添加黑/白名单

参数名称	参数说明	取值样例
地址方向	选择“源地址”或“目的地址”。 • 源地址：设置访问流量中的发送数据包的 IP 地址或 IP 地址组。 • 目的地址：设置访问流量中接收数据包的目的 IP 地址或 IP 地址组。 **说明** **设置后该 IP 地址（组）访问外网的所有地址将只检测但不执行拦截操作，您可以在 3.10 日志审计中检索该 IP 地址（组）查看访问情况和流量情况。**	源地址
IP 地址	支持设置单个 IP 地址、连续多个 IP 地址、地址段。	192.168.10.5
协议类型	协议类型当前支持：TCP、UDP、ICMP、Any。	TCP
端口	“协议类型”选择“TCP”或“UDP”时，设置需要开放或限制的端口。支持设置单个端口或者连续端口组。	单个端口：80 连续端口组：中间使用“-”隔开，如：80-443。

步骤 5 单击“确认”，完成添加。

----结束

3.4.7.2 编辑黑/白名单

如果您想修改已添加的黑/白名单的地址方向、IP 地址、协议类型等配置，可以参考本章节进行重新配置。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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。选择“黑名单”或“白名单”页签。

步骤 4 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，参数详情请参见表 3-7。

表3-7 添加黑/白名单

参数名称	参数说明	取值样例
地址方向	选择“源地址”或“目的地址”。 • 源地址：设置访问流量中的发送数据包的 IP 地址或 IP 地址组。 • 目的地址：设置访问流量中接收数据包的目的 IP 地址或 IP 地址组。 **说明** **设置后该 IP 地址（组）访问外网的所有地址将只检测但不执行拦截操作，您可以在 3.10 日志审计中检索该 IP 地址（组）查看访问情况和流量情况。**	源地址
IP 地址	支持设置单个 IP 地址、连续多个 IP 地址、地址段。	192.168.10.5
协议类型	协议类型当前支持：TCP、UDP、ICMP、Any。	TCP
端口	“协议类型”选择“TCP”或“UDP”时，设置需要开放或限制的端口。支持设置单个端口或者连续端口组。	单个端口：80 连续端口组：中间使用“-”隔开，如：80-443。

步骤 5 修改完成后，单击“确认”保存。

----结束

3.4.7.3 删除黑/白名单

本章节指导您对已添加的黑/白名单进行删除的操作。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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。选择“黑名单”或“白名单”页签。

步骤 4 在需要删除的规则所在行的“操作”列，单击“删除”。

步骤 5 在弹出的“删除黑名单”或“删除白名单”界面，单击“是”，完成删除。

⚠ 警告

删除名单后无法恢复，请谨慎操作。

----结束

3.4.8 配置 DNS 解析

选择默认 DNS 服务器或者添加 DNS 服务器地址，域名防护策略将会按照您配置的域名服务器进行 IP 解析并下发。

当前帐号拥有多个防火墙时，DNS 解析操作会应用于帐号下的所有防火墙。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 > 互联网边界”页面，选择“DNS 解析”页签。

步骤 4 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 5 单击“应用”，完成配置。

说明

当前帐号拥有多个防火墙时，DNS 解析操作会应用于帐号下的所有防火墙。

----结束

3.5 管理 IP 地址组

3.5.1 添加 IP 地址组

IP 地址组是多个 IP 地址的集合。通过使用 IP 地址组，可帮助您有效应对需要重复编辑访问规则的场景，方便批量管理这些访问规则。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“访问控制 > IP 地址组管理”，进入“IP 地址组管理”界面。

步骤 4 单击“添加 IP 地址组”，弹出“基本信息”界面，填写参数如表 3-8 所示。

表3-8 添加 IP 地址组的参数说明

参数	说明
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。
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 5 确认无误后，单击“确认”，完成添加 IP 地址组。

----结束

后续操作

3.5.2 添加 IP 地址。

3.5.2 添加 IP 地址

本文指导您向 IP 地址组中添加 IP 地址。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“访问控制 > IP 地址组管理”，进入“IP 地址组管理”界面。

步骤 4 单击添加的 IP 地址组名称，弹出“基本信息”和“IP 地址列表”界面。

步骤 5 单击“IP 地址列表”界面下的“添加 IP 地址”，弹出“添加 IP 地址”界面。

- 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。
- 添加单个 IP 地址：在列表中单击“添加”，输入“IP 地址”和“描述”信息。

表3-9 添加 IP 地址的参数说明

参数	说明	取值样例
IP 地址	支持设置单个 IP 地址、连续多个 IP 地址、地址段，例如 10.1.1.1、10.1.1.2/24 或 10.1.1.1-10.1.1.2。	10.1.1.1
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。	-

步骤 6 在“添加 IP 地址”界面，单击 ⊕ 添加 可添加多个 IP 地址。

步骤 7 确认信息无误后，单击“确认”，完成添加 IP 地址。

----结束

3.5.3 删除 IP 地址组

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“访问控制 > IP 地址组管理”，进入 IP 地址组管理界面。

步骤 4 在需要删除的 IP 地址组所在行的“操作”列，单击“删除”。

步骤 5 在弹出的“删除 IP 地址组”界面，单击“是”，完成删除。

警告

删除 IP 地址组后无法恢复，请谨慎操作。

----结束

3.6 管理服务组

3.6.1 添加服务组

服务组是多个服务（协议、源端口、目的端口）的集合。通过使用服务组，可帮助您有效应对需要重复编辑访问规则的场景，并且方便管理这些访问规则。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“访问控制 > 服务组管理”，进入“服务组管理”界面。

步骤 4 单击“添加服务组”，弹出“基本信息”界面，填写服务组名称及描述。

表3-10 添加服务组的参数说明

参数	说明
服务组名称	需要添加的服务组名称。
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 5 确认填写信息无误后，单击“确认”，完成添加服务组。

----结束

后续操作

3.6.2 添加服务。

3.6.2 添加服务

本文指导您向服务组中添加服务（协议、源端口、目的端口）。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“访问控制 > 服务组管理”，进入“服务组管理”界面。

步骤 4 单击添加的服务组名称。弹出“基本信息”和“服务列表”。

步骤 5 单击“服务列表”下的“添加服务”，弹出“添加服务”对话框。

表3-11 添加服务

参数名称	参数说明	取值样例
服务名称	需要添加的服务名称，由您定义。	test
协议	协议类型当前支持：TCP、UDP、ICMP、ICMPV6、Any。	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	80
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	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 6 在“添加服务”界面，单击 ⊕ 添加 可添加多个服务。

步骤 7 确认无误后，单击“确认”，完成添加。

----结束

3.6.3 删除服务组

服务组是多个端口的集合。通过使用服务组，可帮助您便捷防御高危端口，有效应对需要重复编辑访问规则的场景，并且方便管理这些访问规则。

删除服务组

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“访问控制>服务组管理”，进入“服务组管理”界面。

步骤 4 在待删除的服务组所在行的“操作”列，单击“删除”。

步骤 5 在弹出的“删除服务组”界面，确认删除的信息无误后，单击“是”，完成删除。

⚠ 警告

删除服务组后无法恢复，请谨慎操作。

----结束

3.7 配置入侵防御策略

您可以配置入侵防御模式，选择防护模式为仅检测并记录日志，或对攻击流量进行自动拦截，助您灵活防御云平台。CFW 为您提供基础防御功能，结合多年攻防实战积累的经验规则，针对访问流量进行检测与防护，可覆盖常见的网络攻击并有效保护资产。

云防火墙默认提供“基础防御”功能，该功能不支持关闭，主要进行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 活动及其他可疑行为。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“入侵防御”。

表3-12 入侵防御功能介绍

功能名称	功能说明
防护模式	• **观察模式**：仅对攻击事件进行检测并记录到日志中。 • **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

功能名称	功能说明
	需求。 – 拦截模式-严格：防护粒度精细，全量拦截攻击请求。建议您等待业务运行一段时间后，根据防护效果配置误报屏蔽规则，再开启“严格”模式。
基础防御	为您的资产提供基础的防护能力，默认“开启”状态。防御功能包括： • 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 活动及其他可疑行为。
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。

----结束

3.8 管理基础防御规则

3.8.1 查看 IPS 规则库

云防火墙默认提供“基础防御”功能，该功能不支持关闭，主要进行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 活动及其他可疑行为。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“入侵防御”。单击“基础防御”中的“查看规则”，进入“基础防御规则”页面。

步骤 4 参数说明如表 3-13 所示。

图3-1 基础防御规则

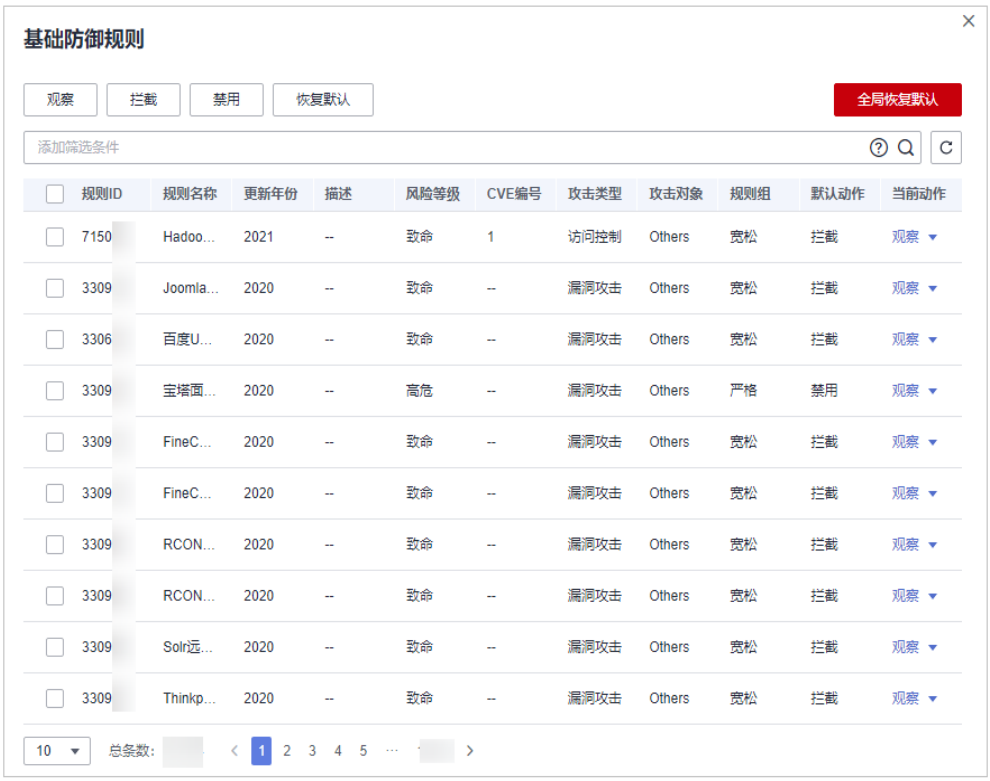

表3-13 基础防御规则参数说明

参数名称	参数说明
规则 ID	防御规则的 ID。
规则名称	防御规则的名称。
更新年份	防御规则的更新年份。
描述	防御规则的描述。
风险等级	防御规则的风险等级，分为低危、中危、高危和致命四种等级。
CVE 编号	防御规则的 CVE 编号。
攻击类型	检测到的攻击类型，包括漏洞攻击、访问控制、黑客工具等。
攻击对象	检测到受“攻击类型”攻击的对象。
规则组	防御规则所属规则组，分为观察、宽松、中等和严格，对应“防护模式”中的四种模式。
默认动作	当前防御规则的默认动作，由当前“防护模式”决定，分为观察、拦截、禁用。
当前动作	云防火墙对匹配当前防御规则流量的操作。

参数名称	参数说明
	若单击“全局恢复默认”，可将列表中所有规则的“当前动作”恢复至与“默认动作”一致。 • 观察：云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：云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：云防火墙对匹配当前防御规则的流量，不记录、不拦截。

步骤 5 （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。

----结束

3.8.2 修改基础防御规则动作

云防火墙默认提供“基础防御”功能，该功能不支持关闭，主要进行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 活动及其他可疑行为。

约束条件

- “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”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“入侵防御”。单击“基础防御”中的“查看规则”，进入“基础防御规则”页面。

步骤 4 （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 5 单击待修改动作的“当前动作”列，选择对应动作。

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

图3-2 修改当前动作

说明

- 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”。
- 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”。

----结束

3.9 流量分析

您可以查看网络中的访问状态，分为 Internet 访问和主动外联访问中业务出入 Internet 边界出入口流量的、攻击趋势等，包括：Internet 访问、主动外联等。可为您提供“近 1 小时”、“近 24 小时”、“近 7 天”的流量分析结果。

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。

前提条件

- 需开启弹性公网 IP 防护，操作步骤请参见 3.3.1 开启弹性公网 IP 防护。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航栏中，选择“流量分析”，进入“流量分析”页面，您可在页面上方选择查看的页签：

- Internet 访问：查看不同时间段互联网总出入口流量、攻击趋势和 TOP 前 10 的访问 IP。参数介绍请参见表 3-14。
- 主动外联访问：查看不同时间段主动外联的出入口流量以及攻击趋势。参数介绍请参见表 3-15。

表3-14 Internet 访问参数介绍

参数名称	参数说明
开放公网 IP	公网 IP 的总个数。 • 风险 IP：呈现为红色，即未开启防护的公网 IP。 • 防护 IP：呈现为蓝色，即已开启防护的公网 IP。
互联网出入口流量	出入互联网的流量统计。
攻击趋势	每个时间节点受到的攻击次数。
TOP 访问 IP	云防火墙检测到的弹性公网 IP 中前 10 个访问率最高的排序。

表3-15 主动外联访问参数介绍

参数名称	参数说明
外联流量统计	主动外联的流量统计。
攻击趋势	每个时间节点对应有多少次攻击。

----结束

3.10 日志审计

3.10.1 日志查询

日志查询为您提供 7 天的日志记录。您可通过攻击事件日志查看检测到的危险流量的危险等级、受影响的端口、命中的规则、攻击事件类型等信息；通过访问控制日志查看根据访问控制策略放行或阻断的所有流量，以便更好的调整访问控制策略；通过流量日志查看通过的所有流量记录。

日志支持筛选、刷新、导出、显示/隐藏列的方式，助您使用。

前提条件

- 3.3.1 开启弹性公网 IP 防护。
- 3.7 配置入侵防御策略。

攻击事件日志

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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，可查看近一周的攻击事件详情。

表3-16 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。
攻击事件类型	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：高、中、低。
规则 ID	对应规则的 ID 号。
命中规则名称	规则库中相对应的命中规则名称。
源 IP	单个 IP 地址、连续多个 IP 地址、地址段。
源端口	攻击事件的源端口。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	单个 IP 地址、连续多个 IP 地址、地址段。
目的端口	攻击事件的目的端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
协议/应用	攻击事件的协议类型，或是什么应用。
方向	包括两个方向：出方向、入方向。
响应动作	包括观察者模式（“观察”）和拦截模式（“阻断”或“放行”）。

----结束

访问控制日志

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在左侧导航树中，选择“日志审计 > 日志查询”。选择“访问控制日志”页签，可查看近一周的访问控制情况。若需要修改指定 IP 访问控制的响应动作，请参照 3.4.1 添加防护规则或 3.4.7.1 添加黑/白名单。

表3-17“访问控制日志”的参数说明

参数	说明
接收时间	访问发生的时间。
访问源	访问的源 IP 地址。
源端口	攻击事件的源端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
访问目的	访问的目的 IP。
目的端口	攻击事件的目的端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
协议	攻击事件的协议类型。
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。
状态	访问控制的状态。

----结束

流量日志

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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。

表3-18“流量日志”的参数说明

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。

参数	说明
访问源	单个 IP 地址、连续多个 IP 地址、地址段。
源端口	攻击事件的源端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
访问目的	访问的目的 IP。
目的端口	攻击事件的目的端口。包括单个端口，或者连续端口组，中间使用“-”隔开，如：80-443
协议	攻击事件的协议类型。
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

3.11 系统管理

3.11.1 告警通知

设置攻击告警和流量超额预警后，CFW 可将 IPS 攻击日志和流量超额的预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。

前提条件

已开通消息通知服务。

攻击告警

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 在“攻击告警”所在行的“操作”列，单击“编辑” ，设置通知项参数，参数说明如表 3-19 所示。

表3-19 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”，那么当云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。
触发条件	设置触发条件。 **说明** **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 5 单击“确认”，完成通知项设置。

步骤 6 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 在左侧导航树中，单击左上方的 ，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 在“流量超额预警”所在行的“操作”列，单击“编辑” ,设置通知项参数，参数说明如表 3-20 所示。

表3-20 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。
通知等级	选择触发通知的流量等级，当流量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。

参数名称	参数说明
通知时间	选择通知的时间段。
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 5 单击“确认”，完成通知项设置。

步骤 6 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

4 常见问题

4.1 产品咨询类

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 云防火墙支持跨帐号使用吗？

云防火墙不支持跨帐号使用。用户仅能使用并管理当前帐号下的云防火墙资源。

4.1.3 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 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，同时支持按需弹性扩容、AI 提升智能防御能力、灵活扩展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。 • 支持对 Web 攻击的基础防护。	• 针对域名或 IP，云上或云下的 Web 业务。

类别	云防火墙	Web 应用防火墙
	• 支持外部入侵和主动外联的流量防护。	• 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：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。

4.1.4 QPS 高，流量峰值就高吗？

QPS 高，流量峰值不一定高。流量峰值根据源站的带宽估计。

4.2 功能类

4.2.1 通过日志审计功能可查看哪些信息？

在“日志审计”页面，可以详细查看每一条用户攻击信息，包括攻击发生时间、攻击类型、危险等级、源端口、源 IP、目的 IP、目的端口等信息。

4.2.2 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。。

4.2.3 云防火墙攻击日志，为什么显示还未纳入防护的 EIP？

云防火墙会将所有受到攻击的 EIP 信息做收集，以便您更好的配置防御策略。

4.3 故障排查类

4.3.1 流量分析页面发现流量日志和攻击日志不全怎么办？

CFW 只记录云防火墙基础版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。

4.3.2 配置了策略为什么没有生效？

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 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 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 4 配置全局阻断规则。单击“添加规则”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。

- “源地址”：0.0.0.0/0
- “目的地址”：0.0.0.0/0
- “源端口”：0-65535
- “目的端口”：0-65535
- “动作”：阻断

说明

建议您添加完所有规则后再开启“启用状态”。

步骤 5 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 6 将步骤 4 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 7 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？

云防火墙中设置的防护策略是根据“弹性公网 IP 管理列表”执行的，若您已开启全局（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 是否在列表中，若不在，需进行资产同步操作，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》。

4.3.3 Apache Log4j 远程代码执行漏洞攻击，云防火墙如何启用检测和防御？

Apache Log4j2 存在一处远程代码执行漏洞（CVE-2021-44228），在引入 Apache Log4j2 处理日志时，会对用户输入的内容进行一些特殊的处理，攻击者可以构造特殊的请求，触发远程代码执行。目前 POC 已公开，风险较高。

12 月 16 日，官方披露低于 2.16.0 版本除了存在拒绝服务漏洞外，还存在另一处远程代码执行漏洞（CVE-2021-45046）。

Apache Log4j2 是一款业界广泛使用的基于 Java 的日志记录工具。云提醒使用 Apache Log4j2 的用户尽快安排自检并做好安全加固。

云防火墙 CFW 已支持检测和拦截 Apache Log4j2 远程代码执行漏洞。

漏洞名称

Apache Log4j 远程代码执行漏洞。

影响范围

影响版本：

2.0-beat9 <= Apache Log4j 2.x < 2.16.0（2.12.2 版本不受影响）。

已知受影响的应用及组件：spring-boot-starter-log4j2/Apache Solr/Apache Flink/Apache Druid。

安全版本：

Apache Log4j 1.x 不受影响。

Apache Log4j 2.16.0。

防护建议

步骤 1 登录 CFW 控制台，在 CFW 页面建议操作如下：

1. 需要购买云防火墙 CFW 服务的**标准版**。
2. 启用入侵防御的**基础防御**功能，并开启**拦截模式**。请参考《云防火墙用户指南》中《配置入侵防御策略》。

----结束

4.3.4 Spring Framework 远程代码执行漏洞攻击，云防火墙如何启用检测和防御？

Spring 是一款主流的 Java EE 轻量级开源框架，面向服务器端开发设计。近日，Spring 框架被曝出可导致 RCE 远程代码执行的漏洞（CVE-2022-22965），该漏洞攻击面较广，潜在危害严重，对 JDK 9 及以上版本皆有影响。

云防火墙 CFW 已支持检测和拦截 Spring Framework 远程代码执行的漏洞攻击。

漏洞名称

Spring Framework 远程代码执行漏洞。

影响范围

- JDK 9 及以上的。
- 使用了 Spring 框架或衍生框架。

防护建议

步骤 1 登录 CFW 控制台，在 CFW 页面建议操作如下：

1. 需要购买云防火墙 CFW 服务的**标准版**。
2. 启用入侵防御的**基础防御**功能，并开启**拦截模式**。请参考《云防火墙用户指南》中《配置入侵防御策略》。

----结束

4.4 网络流量类

4.4.1 流量分析功能有哪些？

在云防火墙流量分析页面，可以查看用户资产互联网出入口流量和攻击趋势，可选择查看时间区间为“近 1 小时”、“近 24 小时”和“近 7 天”的数据。

4.4.2 云防火墙数据流量怎么统计？

目前云防火墙是基于会话的流量统计，在连接期间，数据不会上报，须连接结束后才会上报。

说明

- 流量的大小是基于从会话创建到结束期间该会话的整体流量。
- Internet 互联网边界包括两个方向的流量，即从互联网访问服务的流量和业务主动外联访问的流量。

4.4.3 单条流量超速，需要升级带宽吗？

CFW 流量带宽是针对客户下所有流量，要求整体带宽不超速。如果整体带宽超速会产生预警，整体带宽超速可能会丢包。单条流超速了，总的带宽没有超速，需要先升级带宽，才能保证整体带宽不超速。扩容可防护流量峰值请参考《云防火墙用户指南》中《云防火墙控制台概览》。

4.4.4 云防火墙提供的防护带宽流量是多少？

云防火墙为您提供互联网边界的防护，您可根据需要扩展防护流量带宽。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 10 Mbps/月。

说明

防护带宽流量按照出流量或入流量的最大峰值取值。

4.5 计费类

4.5.1 云防火墙如何收费和计费？

云防火墙**标准版**支持包年/包月（预付费）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。

- 有关 CFW 详细的计费说明，请参见。

4.5.2 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。
  保留期的时长由“客户等级”来定。

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 在左侧导航树中，单击左上方的 ☰，选择“安全 > 云防火墙”，进入云防火墙的概览页面。

步骤 3 在界面右上角，单击“续费”。

步骤 4 在“续费管理”界面，根据页面提示完成续费。

----结束

4.5.3 如何退订云防火墙？

该任务指导用户退订包年/包月方式购买的云防火墙。

退订后原 CFW 配置数据将不能保存，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 3.4.2 批量管理防护规则。

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
2023-05-23	第二次正式发布。 新增以下章节： • 1.4 使用限制。 • 1.5 术语解释。 • 2 计费说明。 • 4.5 计费类。
2023-03-07	第一次正式发布。