

云防火墙

# 用户指南

文档版本 01  
发布日期 2024-12-05



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

# 目录

<b>1 产品介绍</b>	<b>1</b>
1.1 什么是云防火墙	1
1.2 功能特性	2
1.3 应用场景	3
1.4 服务版本差异	4
1.5 权限管理	5
1.6 约束与限制	6
1.7 与其它服务的关系	8
1.8 基本概念	9
<b>2 查看防护总览</b>	<b>11</b>
<b>3 创建云防火墙</b>	<b>14</b>
<b>4 开启互联网边界流量防护</b>	<b>16</b>
<b>5 开启 VPC 边界流量防护</b>	<b>18</b>
5.1 VPC 边界防火墙概述	18
5.2 虚拟私有云模式	18
5.2.1 创建防火墙（虚拟私有云模式）	18
5.2.2 管理防护 VPC	19
5.2.3 配置 VPC 侧路由	21
5.2.4 开启/关闭 VPC 边界防火墙（虚拟私有云）	21
<b>6 配置访问控制策略管控流量</b>	<b>23</b>
6.1 访问控制策略概述	23
6.2 通过配置防护规则拦截/放行流量	24
6.2.1 通过添加防护规则拦截/放行流量	24
6.2.2 示例一：放行入方向中指定 IP 的访问流量	34
6.2.3 示例二：拦截某一地区的访问流量	35
6.3 通过添加黑白名单拦截/放行流量	35
6.4 通过策略助手查看防护信息	37
6.5 访问控制策略管理	37
6.5.1 导入/导出防护策略	38
6.5.2 调整防护规则的优先级	44
6.5.3 管理防护规则	45

6.5.4 管理黑白名单.....	47
6.6 IP 地址组管理.....	48
6.6.1 添加自定义 IP 地址组和 IP 地址.....	48
6.6.2 查看预定义地址组.....	50
6.6.3 删除自定义 IP 地址组.....	51
6.7 域名组管理.....	51
6.7.1 添加域名组.....	51
6.7.2 删除域名组.....	54
6.8 服务组管理.....	54
6.8.1 添加自定义服务组和服务.....	54
6.8.2 查看预定义服务组.....	56
6.8.3 删除自定义服务组.....	57
<b>7 拦截恶意攻击.....</b>	<b>58</b>
7.1 攻击防御功能概述.....	58
7.2 拦截网络攻击.....	60
7.3 拦截病毒文件.....	62
7.4 IPS 规则管理.....	63
7.4.1 修改入侵防御规则的防护动作.....	63
7.4.2 自定义 IPS 特征.....	64
<b>8 查看流量数据.....</b>	<b>69</b>
8.1 查看入云流量.....	69
8.2 查看出云流量.....	70
8.3 查看 VPC 间访问流量.....	71
<b>9 查看云防火墙防护日志.....</b>	<b>73</b>
9.1 日志查询.....	73
<b>10 系统管理.....</b>	<b>77</b>
10.1 告警通知.....	77
10.2 DNS 服务器配置.....	79
10.3 安全报告管理.....	80
10.3.1 创建安全报告.....	80
10.3.2 查看/下载安全报告.....	81
10.3.3 管理安全报告.....	82
<b>11 常见问题.....</b>	<b>84</b>
11.1 产品咨询.....	84
11.1.1 云防火墙支持线下服务器吗? .....	84
11.1.2 云防火墙支持跨账号使用吗? .....	84
11.1.3 云防火墙与 Web 应用防火墙有什么区别? .....	84
11.1.4 云防火墙和安全组、网络 ACL 的访问控制有什么区别? .....	85
11.1.5 云防火墙支持哪些维度的访问控制? .....	86
11.1.6 云防火墙的防护顺序是什么? .....	86

11.1.7 是否支持同时部署 WAF 和 CFW? .....	87
11.2 故障排查.....	88
11.2.1 业务流量异常怎么办? .....	88
11.2.2 流量日志和攻击日志信息不全怎么办? .....	92
11.2.3 防护规则没有生效怎么办? .....	92
11.2.4 IPS 拦截了正常业务如何处理? .....	93
11.2.5 为什么访问控制日志页面数据为空? .....	94
11.3 网络流量.....	94
11.3.1 云防火墙数据流量怎么统计? .....	94
11.3.2 流量趋势模块和流量分析页面展示的流量有什么区别? .....	94
11.3.3 如何验证 HTTP/HTTPS 的出方向域名防护规则的有效性? .....	95
<b>A 修订记录.....</b>	<b>96</b>

# 1 产品介绍

## 1.1 什么是云防火墙

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。

### 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。
- 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“标准版”、“专业版”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
总览	提供防火墙实例基本信息、资源防护总览、统计信息等内容。
资产管理	管理、查看弹性公网IP和VPC的相关数据及信息。
访问控制	<ul style="list-style-type: none"><li>支持基于IP、域名、地域等方式对互联网边界和VPC边界流量进行访问控制。</li><li>支持通过“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。</li></ul>
攻击防御	<ul style="list-style-type: none"><li>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，覆盖多种常见的网络攻击，有效保护您的资产。<ul style="list-style-type: none"><li>基础防御规则库：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。 <b>说明</b> 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。</li><li>虚拟补丁规则库：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。虚拟补丁规则库中展示新增的IPS规则；防火墙新增IPS规则时，会先进入虚拟补丁规则库中，防护一段时间后合入IPS规则库中。</li><li>自定义IPS特征：当IPS规则库不满足使用时，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。 <b>说明</b> 自定义IPS特征支持添加HTTP、TCP、UDP、POP3、SMTP、FTP的协议类型。</li></ul></li><li>“敏感目录扫描防御”：防御对用户主机敏感目录的扫描攻击。</li><li>“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。</li><li>病毒防御（Anti-Virus，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。</li></ul>

功能项	功能描述
流量分析	为您展示以下流量统计情况。 <ul style="list-style-type: none"><li>入云流量：互联网访问云主机的流量统计。</li><li>出云流量：云主机主动访问互联网的流量统计。</li><li>VPC间访问：VPC间的出入流量统计。</li></ul>
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： <ul style="list-style-type: none"><li>攻击事件日志：入侵攻击事件的详细信息。</li><li>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。</li><li>流量日志：可以查看具体某个业务的访问流量信息。</li></ul>
系统管理	<ul style="list-style-type: none"><li>告警通知：您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您设置的接收通知方式（例如邮件或短信）发送给您。</li><li>DNS配置：通过域名服务器解析并下发IP地址。</li><li>安全报告：生成日志报告，及时掌握资产的安全状况数据。</li></ul>

表 1-2 引擎特性

名称	主要功能描述	支持协议	支持场景
防火墙引擎	用户流量先经过负载均衡组件分发给租户防火墙引擎，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	可以支持互联网边界和VPC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管控。

### VPC 间互访控制（专业版支持）

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》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 服务版本差异

云防火墙提供了“标准版”、“专业版”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。

详细的功能介绍请参见[功能特性](#)，具体差异请参见表 [版本差异说明](#)。

表 1-3 版本差异说明

功能		标准版	专业版
防护对象	IPv4	√	√
	IPv6	×	×
访问流量控制	公网资产ACL访问控制（基于IP、域名、域名组、地理位置等）	√	√
	南北向流量防护，统一隔离防护云上资产在互联网的暴露风险（例如EIP）	√	√
	南北向流量审计，日志查询	√	√
	东西向流量防护，VPC间的资产保护、全流量分析	×	√
	东西向流量监控，实时获取VPC间流量数据	×	√
防护策略	入侵防御IPS	√	√
	自定义IPS特征库	×	√
	虚拟补丁	√	√
	敏感目录、反弹Shell	√	√
	病毒防御AV	×	√
系统管理	多账号管理	20个	50个

## 📖 说明

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。

## 1.5 权限管理

如果您需要对云服务平台上购买的云防火墙（CFW）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制员工对云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些员工拥有云防火墙（CFW）的使用权限，但是不希望这些员工拥有删除CFW等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CFW，但是不允许删除CFW的权限策略，控制员工对CFW资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CFW服务的其它功能。

## CFW 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CFW部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问CFW时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其它角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CFW服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表1-4所示，包括了CFW下所有的系统角色。

表 1-4 CFW 系统角色

角色名称	描述	类别	依赖关系
CFW FullAccess	云防火墙服务的所有权限。	系统策略	无

角色名称	描述	类别	依赖关系
CFW ReadOnlyAccess	云防火墙服务的只读权限。	系统策略	无

## CFW FullAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "cfw:*:*",
      "vpc:publicIps:list"
    ]
  }]
}
```

## CFW ReadOnlyAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "cfw:*:list",
      "cfw:*:get",
      "vpc:publicIps:list"
    ]
  }]
}
```

# 1.6 约束与限制

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，不支持全域公网带宽GEIP、API网关APIG绑定的EIP的流量防护。
- 云防火墙不支持防护中文域名。

## 防护策略配额限制

- 防护规则
  - 一个防火墙实例最多添加20000条防护规则。
- 黑白名单
  - 一个防火墙实例最多添加2000条黑名单。
  - 一个防火墙实例最多添加2000条白名单。
- 成员组
  - IP地址组

- 每个防火墙实例下最多添加3800个IP地址组。
- 每个IP地址组中最多添加640个IP地址成员。
- 每个防火墙实例下最多添加30000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40000次，泛域名被“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。
  - **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。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。
- 单个日志单次最多支持导出100,000条记录。

## 1.7 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。

### 与消息通知服务的关系

消息通知服务（Simple Message Notification，SMN）提供消息通知功能。用户在CFW开启通知设置后，资源受到攻击或防护流量超额时，会通过设置的接收通知方式收到告警信息。

### 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1-5](#)所示。

表 1-5 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	<ul style="list-style-type: none"><li>弹性公网IP和VPC边界。</li><li>支持对Web攻击的基础防护。</li><li>支持外部入侵和主动外联的流量防护。</li></ul>	<ul style="list-style-type: none"><li>针对域名或IP，云上或云下的Web业务。</li><li>支持对Web攻击的全面防护。</li></ul>
功能特性	<ul style="list-style-type: none"><li>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。</li><li>访问控制：支持互联网边界访问流量的访问控制。</li><li>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。</li></ul>	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。

## 1.8 基本概念

### 五元组

五元组包括：源IP地址、目的IP地址、协议号、源端口、目的端口。

### 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。

## 互联网边界防火墙

互联网边界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。

## 入侵防御系统

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。

## 病毒防御

病毒防御（Anti-Virus, 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。

## 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。

## 对等连接

对等连接是指两个VPC之间的网络连接。使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。同一资源池内，可以在自己的VPC之间创建对等连接，也可以在自己的VPC与其他用户的VPC之间创建对等连接。不同资源池的VPC之间不能创建对等连接。

## CVE 编号

CVE编号是识别漏洞的唯一标识符。

CVE (Common Vulnerabilities and Exposures, 通用漏洞披露) 是安全漏洞列表，列表中的每个条目都会有一个唯一的CVE编号。

## 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

# 2 查看防护总览


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，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[VPC边界防火墙](#)后才能查看。

## 查看概览

**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 CFW”，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 防火墙实例信息](#)。

表 2-1 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。
版本规格	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。




参数名称	参数说明
操作	支持查看详情等操作。

**步骤4** 在“资源防护概况”中，查看当前账号的当前区域下所有云资源（EIP、VPC）的防护状态。

**步骤5** 查看防火墙实例详细信息。

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 [表 防火墙实例详细信息](#) 所示。

表 2-2 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”两种版本。
	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	防护EIP数	当前防火墙实例防护的弹性公网IP数量。
	总防护VPC数量	当前防火墙实例可防护的VPC总数。
	CFW实例规格	当前防火墙实例的规格。
	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。
其他信息	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和跟踪。

**步骤6** 在“运营看板”模块，查看云资源总体防护数据。

切换“互联网边界”和“VPC边界”，查看对应场景的总体防护数据。

在右上角切换查询时间。

- 查看访问控制策略的拦截效果，以及出/入方向流量的最大值。
- 流量趋势：查看出/入方向和整体的流量变化趋势。

表 2-3 取值说明

时间段	平均值取	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

#### 说明

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。
- 访问控制：查看访问控制策略阻断或放行的防护情况。

----结束

# 3 创建云防火墙

云防火墙支持一个区域下创建多个防火墙，便于管理不同场景下的资源和策略。

## 前提条件

当前账号拥有BSS Administrator和CFW FullAccess权限。

## 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[服务版本差异](#)。

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 CFW”，进入云防火墙的总览页面。

**步骤3** 单击“创建云防火墙”，进入“创建云防火墙”页面，相关参数如[表3-1](#)所示。

**表 3-1** 创建云防火墙的参数说明

参数名称	参数说明
计费模式	云防火墙实例支持包年/包月计费模式。
区域	根据防护业务的所在区域选择。
版本规格	选择版本：标准版。


参数名称	参数说明
可用区	选择区域中的可用区。
防火墙名称	设置云防火墙实例的名称。
防护带宽	选择实例的防护带宽值。
实例规格	选择实例的规格。

**步骤4** 确认信息无误后，单击“创建云防火墙”。

----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 CFW”，进入云防火墙的总览页面。

**步骤3** 单击“创建云防火墙”，进入“创建云防火墙”页面，相关参数如表 [创建云防火墙的参数说明](#) 所示。

表 3-2 创建云防火墙的参数说明

参数名称	参数说明
计费模式	云防火墙实例支持包年/包月计费模式。
区域	根据防护业务的所在区域选择。
版本规格	选择版本：专业版。
可用区	选择区域中的可用区。
防火墙名称	设置云防火墙实例的名称。
防护带宽	选择实例的防护带宽值。
实例规格	选择实例的规格。

**步骤4** 确认信息无误后，单击“创建云防火墙”。

----结束

# 4 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。

您需配置访问控制策略或IPS防护模式，云防火墙才会实施拦截操作，配置访问控制策略请参见[添加防护规则](#)，IPS相关请参见[配置入侵防御策略](#)。

## 约束条件

- 弹性公网IP防护目前不支持IPv6防护。
- 一个EIP只能在一个防火墙上开启防护。
- 仅支持当前账号所属企业项目下的弹性公网IP。

## 对业务的影响

开启或关闭EIP的防护不会造成业务中断，保证流量平滑切换。


### 须知

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。

- 编辑防护规则请参见[管理防护规则](#)。
- 编辑黑名单请参见[管理黑白名单](#)。

## 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 CFW”，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信息将自动更新至列表中。

**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，单击列表上方的“开启防护”。

**须知**

- 弹性公网IP防护目前不支持IPv6防护。
- 一个EIP只能在一个防火墙上开启防护。
- 仅支持当前账号所属企业项目下的弹性公网IP。

**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****相关操作**

- 关闭弹性公网IP防护：
  - 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”。
- 新增EIP自动防护：在列表上方单击“新增EIP自动防护”，开启后，新增的EIP将自动开启防护，EIP流量将经过防火墙并被防火墙防护。

**后续操作**

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：

- 如果希望实现流量管控，需配置防护策略，请参见[互联网边界防护规则](#)或[通过添加黑白名单拦截/放行流量](#)。
  - 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。
- 如果希望拦截网络攻击，请参见[拦截网络攻击](#)。

# 5 开启 VPC 边界流量防护

## 5.1 VPC 边界防火墙概述

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

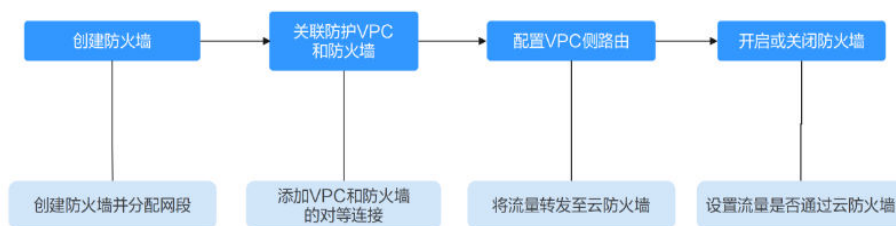
### 约束条件

- 仅“专业版”支持VPC边界防火墙。
- 仅支持防护当前账号所属企业项目下的VPC。

### 配置流程

下图为虚拟私有云关联模式的配置流程：

图 5-1 虚拟私有云关联模式配置流程



## 5.2 虚拟私有云模式

### 5.2.1 创建防火墙（虚拟私有云模式）


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。

## 约束条件

仅“专业版”支持VPC边界防火墙。

## 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 在左侧导航栏中，单击左上方的，选择“安全 > 云防火墙 CFW”，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** 配置合适的网段，将默认自动创建Inspection VPC。

### 说明

请您在进行网络规划时注意以下事项：

- 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。

**步骤7** 单击“确认”，完成VPC间防火墙的创建。

----结束

## 5.2.2 管理防护 VPC

创建VPC边界防火墙后，您需将VPC关联至防火墙，请参见[关联防护VPC和防火墙](#)。


无需防护某个VPC时，需将VPC解除与防火墙的关联，请参见[解除防护VPC和防火墙的关联](#)。

## 约束条件

解除防护VPC与防火墙的关联时，需优先删除[配置VPC侧路由](#)中指向防火墙的路由。

## 关联防护 VPC 和防火墙

**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 CFW”，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** 在列表中，单击待防护VPC“操作”列的“关联防火墙”。

**步骤6** 在“关联防火墙”页面，填写参数如表 添加防护VPC页面参数所示。

表 5-1 添加防护 VPC 页面参数


参数名称	参数说明	
防护类型	不支持修改，默认为“虚拟私有云”。	
虚拟私有云	当前被防护VPC的名称和网段。	
防火墙侧路由	被防护VPC网段	默认填写“虚拟私有云”选择的VPC的网段，如有需要可修改或单击  添加 添加网段。
	下一跳类型	不支持修改，默认为“对等连接”。
	下一跳	不支持修改，VPC通过此对等连接将流量转发至防火墙。
	描述	(可选)自定义防护VPC的描述信息。
路由配置	配置VPC侧路由	勾选后，防火墙将在该VPC的所有路由表中添加指向10.0.0.0/8、172.16.0.0/12、192.168.0.0/16，下一跳为云防火墙对等连接的路由。 <b>注意</b> 建议在确认不会对您现有的网络造成影响后勾选。

**步骤7** 单击“确认”，完成防护VPC和防火墙的关联。

----结束

## 解除防护 VPC 和防火墙的关联

**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 CFW”，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** 在列表中，待解除关联VPC所在行的“操作”列中，单击“解除关联”。

**步骤6** 单击确认框中的“确定”后可以解除防护VPC和防火墙的关联。

### 说明

如果被解除关联的VPC存在“下一跳”为指向防火墙的“对等连接”的路由，会无法操作，须删除该路由后才能解除VPC的关联。

----结束

## 后续操作


关联VPC后，需要执行[配置VPC侧路由](#)添加路由。

### 5.2.3 配置 VPC 侧路由

本节指导您配置VPC侧路由。

#### 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“网络 > 虚拟私有云 > 路由表”，进入“路由表”页面。

**步骤3** 在“名称/ID”列，单击对应VPC的路由表名称，进入“基本信息”页面。

**步骤4** 单击“添加路由”，参数详情见[表 添加路由参数说明](#)。

表 5-2 添加路由参数说明

参数	说明
目的地址	目的地址网段。
下一跳类型	在下拉列表中，选择类型“对等连接”。
下一跳	选择下一跳资源为与引流VPC关联的对等连接。
描述	路由的描述信息，非必填项。 <b>说明</b> 描述信息内容不能超过255个字符，且不能包含“<”和“>”。


----结束

### 5.2.4 开启/关闭 VPC 边界防火墙（虚拟私有云）

配置完成后，防火墙默认为“未开启”状态，您可选择手动开启或关闭VPC间防护功能。

#### 开启防火墙

**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 CFW”，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** 在页面上方，单击“防火墙状态”侧“开启防护”。

**步骤6** 单击“确认”，完成开启防火墙。

----结束

## 关闭防火墙

**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 CFW”，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** 在页面上方列表中，单击“防火墙状态”侧的“关闭防护”。

**步骤6** 单击“确认”，完成关闭防火墙。

----结束

## 后续操作

开启防火墙后，如果您需要添加新的防护VPC。需要执行[关联防护VPC和防火墙](#)和[配置VPC侧路由](#)，完成添加。

# 6 配置访问控制策略管控流量

## 6.1 访问控制策略概述

开启防护后，云防火墙默认放行所有流量，配置合适的访问控制策略能有效地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。

### 访问控制策略类型

访问控制策略分为“防护规则”和“黑/白名单”两类功能，区别如表 [防护规则和黑/白名单的区别](#) 所示，流量命中某一条策略时，执行该策略的动作。

表 6-1 防护规则和黑/白名单的区别

类型	支持的防护对象	网络类型	防护后的动作	配置方式
防护规则	<ul style="list-style-type: none"><li>五元组</li><li>IP地址组</li><li>地理位置（地域）</li><li>域名和域名组</li></ul>	<ul style="list-style-type: none"><li>公网IP</li><li>私网IP</li></ul>	<ul style="list-style-type: none"><li>设置为“阻断”：流量直接拦截。</li><li>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。</li></ul>	通过添加防护规则拦截/放行流量
黑名单	<ul style="list-style-type: none"><li>五元组</li></ul>		直接拦截流量。	通过添加黑白名单拦截/放行流量
白名单	<ul style="list-style-type: none"><li>IP地址组</li></ul>		流量被云防火墙放行，不再经过其它功能检测。	

### 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[VPC边界防火墙](#)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。

## 通配符规则

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。
域名	*.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。
服务-源端口/目的端口	80-443	对80到443之间的所有端口生效。
服务-源端口/目的端口	<ul style="list-style-type: none"><li>● 80</li><li>● 443</li></ul>	对80和443端口生效。

## 相关文档

- 添加单个规则实现流量防护，请参见[通过添加防护规则拦截/放行流量](#)，添加单个黑/白名单实现流量防护请参见[通过添加黑白名单拦截/放行流量](#)。
- 批量添加防护策略，请参见[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[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[查看流量数据](#)，详细流量记录请参见[流量日志](#)。

## 6.2 通过配置防护规则拦截/放行流量

### 6.2.1 通过添加防护规则拦截/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。

防护规则支持防护以下几种场景：

- 防护互联网边界中公网资产的流量，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[为什么需要放行回源IP](#)。
- 配置白名单请参见[通过添加黑白名单拦截/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)。ALG能够对应用层数据载荷中的字段进行分析，并针对在载荷中会包含端口和IP地址的多通道协议（例如FTP、SIP等）动态调整策略。但CFW的防护策略仅支持对端口设置静态策略。如果需要允许多通道协议通信，建议配置一条放通所有端口的规则。
- 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20000条防护规则。
  - 单条防护规则最大限制如下：
    - 最多添加20条IP地址（源和目的各20条）。
    - 最多关联2条“IP地址组”（源和目的各2条）。
    - 最多关联5条服务组。
- 域名防护限制：
  - 域名防护时不支持添加中文域名格式。
  - 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[自定义域名服务器](#)。
- 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[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”中，填写新的防护信息，填写规则请参见[表 添加防护规则-互联网边界](#)。



表 6-2 添加防护规则-互联网边界

参数名称	参数说明
规则类型	选择安全策略的防护类型。 <ul style="list-style-type: none"><li>● EIP规则：防护EIP的流量，仅支持配置公网IP；</li><li>● NAT规则：防护NAT的流量，可以配置私网IP。</li></ul>
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： <ul style="list-style-type: none"><li>● 外-内：互联网访问云上资产（EIP）。</li><li>● 内-外：云上资产（EIP）访问互联网。</li></ul>
源	设置访问流量中发送数据的地址参数。 <ul style="list-style-type: none"><li>● 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。<ul style="list-style-type: none"><li>- 单个公网IP地址，如：xx.xx.10.5</li><li>- 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</li><li>- 公网IP地址段，使用“/”隔开掩码，如：xx.xx.2.0/24</li></ul></li><li>● 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<a href="#">添加自定义IP地址组和IP地址</a>，预定义地址组请参见<a href="#">查看预定义地址组</a>。<p><b>说明</b> “方向”配置为“外-内”时，“源”地址支持配置“预定义地址组”。</p></li><li>● 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。</li><li>● Any：任意源地址。</li></ul>

参数名称	参数说明
目的	<p>设置访问流量中的接收数据的地址参数。</p> <ul style="list-style-type: none"><li>● 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。<ul style="list-style-type: none"><li>- 单个公网IP地址，如：xx.xx.10.5</li><li>- 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</li><li>- 公网IP地址段，使用"/"隔开掩码，如：xx.xx.2.0/24</li></ul></li><li>● 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<a href="#">添加自定义IP地址组和IP地址</a>。</li><li>● 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。</li><li>● 域名/域名组：“方向”选择“内-外”时，支持域名或域名组的防护。<ul style="list-style-type: none"><li>- 应用型：支持<b>域名或泛域名</b>的防护；适用应用层协议，支持HTTP、HTTPS的应用协议类型；通过域名匹配。</li><li>- 网络型：支持<b>单个域名或多个域名</b>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。</li></ul></li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>- 防护HTTP、HTTPS应用类型的<b>域名</b>时可选择任意类型。</li><li>- 防护HTTP、HTTPS应用类型的<b>泛域名</b>时仅支持选择“应用型”的任意选项。</li><li>- 防护其它应用类型（如FTP、MySQL、SMTP）的<b>单个域名</b>：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）。</li><li>- 防护其它应用类型（如FTP、MySQL、SMTP）的<b>多个域名</b>：选择“网络型”“网络域名组”。</li><li>- 同一域名同时需要配置HTTP/HTTPS（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”。</li><li>- 应用型与网络型详细介绍请参见<a href="#">添加域名组</a>。</li></ul> <ul style="list-style-type: none"><li>● Any：任意目的地址。</li></ul>



参数名称	参数说明
服务	<ul style="list-style-type: none"><li>● 服务：设置协议类型、源端口和目的端口。<ul style="list-style-type: none"><li>- 协议类型：支持选择TCP、UDP、ICMP。</li><li>- 源/目的端口：“协议类型”选择“TCP”或“UDP”时，需要设置端口号。</li></ul></li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>- 如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。</li><li>- 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”。</li><li>- 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”。</li></ul> <ul style="list-style-type: none"><li>● 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<a href="#">添加自定义服务组和服务</a>，预定义服务组请参见<a href="#">查看预定义服务组</a>。</li><li>● Any：任意协议类型和端口号。</li></ul>
动作	设置流量经过防火墙时的处理动作。 <ul style="list-style-type: none"><li>● 放行：防火墙允许此流量转发。</li><li>● 阻断：防火墙禁止此流量转发。</li></ul>
配置长连接	当前防护规则仅配置一个“服务”且“协议类型”选择“TCP”或“UDP”时，可配置业务会话老化时间。 <ul style="list-style-type: none"><li>● 是：设置长连接时长。</li><li>● 否：保留默认时长，各协议规则默认支持的连接时长如下：<ul style="list-style-type: none"><li>- TCP协议：1800s。</li><li>- UDP协议：60s。</li></ul></li></ul> <p><b>说明</b> 最大支持50条规则设置长连接。</p>
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”。 <p><b>说明</b> 支持时长设置为1秒~1000天。</p>
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。
策略优先级	设置该策略的优先级： <ul style="list-style-type: none"><li>● 置顶：表示将该策略的优先级设置为最高。</li><li>● 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。</li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>● 设置后，优先级数字越小，策略的优先级越高。</li><li>● 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”。</li></ul>

参数名称	参数说明
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。
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。

----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[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 添加防护规则](#)。

**表 6-3** 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	设置访问流量中发送数据的地址参数。 <ul style="list-style-type: none"><li>● IP地址：支持设置单个IP地址、多个连续IP地址、地址段。<ul style="list-style-type: none"><li>- 单个IP地址，如：192.168.10.5</li><li>- 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10</li><li>- 地址段，使用“/”隔开掩码，如：192.168.2.0/24</li></ul></li><li>● IP地址组：支持多个IP地址的集合，添加IP地址组请参见<a href="#">添加IP地址组</a>。</li><li>● Any：任意源地址。</li></ul>

参数名称	参数说明
目的	<p>设置访问流量中的接收数据的地址参数。</p> <ul style="list-style-type: none"><li>● IP地址：支持设置单个IP地址、多个连续IP地址、地址段。<ul style="list-style-type: none"><li>- 单个IP地址，如：192.168.10.5</li><li>- 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10</li><li>- 地址段，使用"/"隔开掩码，如：192.168.2.0/24</li></ul></li><li>● IP地址组：支持多个IP地址的集合，添加IP地址组请参见<a href="#">添加IP地址组</a>。</li><li>● Any：任意目的地址。</li></ul>
服务	<p>设置访问流量的“协议类型”和“端口号”。</p> <ul style="list-style-type: none"><li>● 服务：设置协议类型、源端口和目的端口。<ul style="list-style-type: none"><li>- 协议类型：支持选择TCP、UDP、ICMP。</li><li>- 源/目的端口：“协议类型”选择“TCP”或“UDP”时，需要设置端口号。</li></ul></li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>- 如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。</li><li>- 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”。</li><li>- 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”。</li></ul> <ul style="list-style-type: none"><li>● 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<a href="#">添加服务组</a>，预定义服务组请参见<a href="#">查看预定义服务组</a>。</li><li>● Any：任意协议类型和端口号。</li></ul>
动作	<p>设置流量经过防火墙时的处理动作。</p> <ul style="list-style-type: none"><li>● 放行：防火墙允许此流量转发。</li><li>● 阻断：防火墙禁止此流量转发。</li></ul>
配置长连接	<p>当前防护规则仅配置一个“服务”且“协议类型”选择“TCP”或“UDP”时，可配置业务会话老化时间。</p> <ul style="list-style-type: none"><li>● 是：设置长连接时长。</li><li>● 否：保留默认时长，各协议规则默认支持的连接时长如下：<ul style="list-style-type: none"><li>- TCP协议：1800s。</li><li>- UDP协议：60s。</li></ul></li></ul> <p><b>说明</b> 最大支持50条规则设置长连接。</p>
长连接时长	<p>“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”。</p> <p><b>说明</b> 支持时长设置为1秒~1000天。</p>

参数名称	参数说明
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。
策略优先级	设置该策略的优先级: <ul style="list-style-type: none"><li>● 置顶:表示将该策略的优先级设置为最高。</li><li>● 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。</li></ul> <b>说明</b> <ul style="list-style-type: none"><li>● 设置后,优先级数字越小,策略的优先级越高。</li><li>● 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”。</li></ul>
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。
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。

----结束

## NAT 流量防护规则

**步骤1** 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2** 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。

**表 6-4** 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。 <b>说明</b> NAT规则需满足: <ul style="list-style-type: none"><li>● “专业版”防火墙。</li><li>● 已配置VPC边界防火墙。</li></ul>
名称	自定义安全策略规则的名称。
方向	选择“SNAT”。

参数名称	参数说明
源	<p>设置访问流量中发送数据的地址参数。</p> <ul style="list-style-type: none"><li>● 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。<ul style="list-style-type: none"><li>- 单个IP地址，如：192.168.10.5</li><li>- 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10</li><li>- 地址段，使用"/"隔开掩码，如：192.168.2.0/24</li></ul></li><li>● 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<a href="#">添加自定义IP地址组和IP地址</a>。</li><li>● 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。</li><li>● Any：任意源地址。</li></ul>
目的	<p>设置访问流量中的接收数据的地址参数。</p> <ul style="list-style-type: none"><li>● 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。<ul style="list-style-type: none"><li>- 单个IP地址，如：192.168.10.5</li><li>- 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10</li><li>- 地址段，使用"/"隔开掩码，如：192.168.2.0/24</li></ul></li><li>● 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<a href="#">添加自定义IP地址组和IP地址</a>。</li><li>● 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。</li><li>● 域名/域名组：“方向”选择“内-外”时，支持域名或域名组的防护。<ul style="list-style-type: none"><li>- 应用型：支持<b>域名或泛域名</b>的防护；适用应用层协议，支持HTTP、HTTPS的应用协议类型；通过域名匹配。</li><li>- 网络型：支持<b>单个域名或多个域名</b>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。</li></ul></li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>- 防护HTTP、HTTPS应用类型的<b>域名</b>时可选择任意类型。</li><li>- 防护HTTP、HTTPS应用类型的<b>泛域名</b>时仅支持选择“应用型”的任意选项。</li><li>- 防护其它应用类型（如FTP、MySQL、SMTP）的<b>单个域名</b>：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）。</li><li>- 同一域名同时需要配置HTTP/HTTPS（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”。</li><li>- 应用型与网络型详细介绍请参见<a href="#">添加域名组</a>。</li></ul> <ul style="list-style-type: none"><li>● Any：任意目的地址。</li></ul>

参数名称	参数说明
服务	<ul style="list-style-type: none"><li>● 服务：设置协议类型、源端口和目的端口。<ul style="list-style-type: none"><li>- 协议类型：支持选择TCP、UDP、ICMP。</li><li>- 源/目的端口：“协议类型”选择“TCP”或“UDP”时，需要设置端口号。</li></ul></li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>- 如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。</li><li>- 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”。</li><li>- 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”。</li></ul> <ul style="list-style-type: none"><li>● 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<a href="#">添加自定义服务组和服务</a>，预定义服务组请参见<a href="#">查看预定义服务组</a>。</li><li>● Any：任意协议类型和端口号。</li></ul>
动作	设置流量经过防火墙时的处理动作。 <ul style="list-style-type: none"><li>● 放行：防火墙允许此流量转发。</li><li>● 阻断：防火墙禁止此流量转发。</li></ul>
配置长连接	当前防护规则仅配置一个“服务”且“协议类型”选择“TCP”或“UDP”时，可配置业务会话老化时间。 <ul style="list-style-type: none"><li>● 是：设置长连接时长。</li><li>● 否：保留默认时长，各协议规则默认支持的连接时长如下：<ul style="list-style-type: none"><li>- TCP协议：1800s。</li><li>- UDP协议：60s。</li></ul></li></ul> <p><b>说明</b> 最大支持50条规则设置长连接。</p>
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”。 <p><b>说明</b> 支持时长设置为1秒~1000天。</p>
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。
策略优先级	设置该策略的优先级： <ul style="list-style-type: none"><li>● 置顶：表示将该策略的优先级设置为最高。</li><li>● 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。</li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>● 设置后，优先级数字越小，策略的优先级越高。</li><li>● 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”。</li></ul>

参数名称	参数说明
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。
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3** 单击“确认”，完成配置防护规则。

#### 说明

访问控制策略默认状态为放行。

----结束

## 相关操作

批量添加防护规则请参见[导入/导出防护策略](#)。

## 6.2.2 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[通过添加防护规则拦截/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，设置参数如下，其余参数可根据您的部署进行填写：

- 方向：外-内
- 源：Any
- 目的：Any
- 服务：Any
- 应用：Any
- 动作：阻断

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：

- 方向：外-内
- 源：选择“IP地址”，填写具体放行的IP。
- 目的：Any
- 服务：Any
- 应用：Any
- 动作：放行

### 6.2.3 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[通过添加防护规则拦截/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。

- 方向：外-内
- 源：选择“地域”、“北京”
- 目的：Any
- 服务：Any
- 动作：阻断

## 6.3 通过添加黑白名单拦截/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[导入/导出防护策略](#)。

#### 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[为什么需要放行回源IP](#)。
- 配置防护规则请参见[通过添加防护规则拦截/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IP地址组和IP地址](#)。
  - 添加防护规则请参见[通过添加防护规则拦截/放行流量](#)。
- 私网IP防护，需满足专业版防火墙且开启[VPC边界防火墙](#)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[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 CFW”，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6-5。

表 6-5 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”。 <ul style="list-style-type: none"><li>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。</li><li>目的地址：设置访问流量中接收数据包的IP地址或IP地址组。</li></ul>
协议类型	协议类型当前支持：TCP、UDP、ICMP、Any。
端口	“协议类型”选择“TCP”或“UDP”时，设置需要放行或拦截的端口。 <b>说明</b> <ul style="list-style-type: none"><li>如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。</li><li>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”。</li><li>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”。</li></ul>
描述	设置该黑/白名单的备注信息。
IP地址列表	<ul style="list-style-type: none"><li>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。</li><li>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<a href="#">查看预定义地址组</a>。</li></ul> <b>注意</b> “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。

**步骤6** 单击“确认”，完成添加。

----结束

## 相关操作


- 编辑和删除黑白名单请参见[管理黑白名单](#)。
- 批量添加黑白名单请参见[导入/导出防护策略](#)。

## 6.4 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 CFW”，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 [策略助手可视化统计参数说明](#)。单击单条数据查看策略命中详情，参数说明请参见表 [访问控制日志参数说明](#)。

表 6-6 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

## 6.5 访问控制策略管理

## 6.5.1 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 CFW”，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。

- 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[通过添加黑白名单拦截/放行流量](#)。
- IP地址组参数说明请参见[添加自定义IP地址组和IP地址](#)。
- 服务组参数说明请参见[添加自定义服务组和服务](#)。
- 域名组参数说明请参见[域名组管理](#)。

#### 须知

- 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。

**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 CFW”，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 6-7 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。	test
防护规则	选择安全策略的防护类型。 <ul style="list-style-type: none"><li>EIP防护：防护EIP的流量，仅支持配置公网IP。</li><li>NAT防护：防护NAT的流量，可以配置私网IP。</li></ul>	EIP防护
方向	选择防护方向： <ul style="list-style-type: none"><li>外-内：外网访问内部服务器。</li><li>内-外：客户服务器访问外网。</li></ul>	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”。设置防护的IP类型。	IPv4
启用状态	选择该策略是否立即启用。 <ul style="list-style-type: none"><li>启用：表示立即开启，规则生效；</li><li>禁用：表示关闭，规则不生效。</li></ul>	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。 <ul style="list-style-type: none"><li>● <b>IP地址</b>: 支持设置单个IP地址、连续多个IP地址、地址段。</li><li>● <b>IP地址组</b>: 支持多个IP地址的集合。</li><li>● <b>地域</b>: 支持按照地域防护。</li></ul>	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: <ul style="list-style-type: none"><li>● 单个IP地址, 如: 192.168.10.5</li><li>● 多个连续地址, 中间使用“-”隔开, 如: 192.168.0.2-192.168.0.10</li><li>● 地址段, 使用“/”隔开掩码, 如: 192.168.2.0/24</li></ul> <b>说明</b> 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”。	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
目的地址类型	选择访问流量中的接收数据的地址类型。 <ul style="list-style-type: none"><li>● <b>IP地址</b>: 支持设置单个IP地址、连续多个IP地址、地址段。</li><li>● <b>IP地址组</b>: 支持多个IP地址的集合。</li><li>● <b>域名</b>: 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。</li><li>● <b>域名组</b>: 支持多个域名的集合。</li><li>● <b>地域</b>: 支持地域防护。</li></ul>	IP地址组

参数名称	参数说明	取值样例
目的IP地址	<p>“目的地址类型”选择“IP地址”时，需填写“目的IP地址”。</p> <p>目的IP地址支持以下输入格式：</p> <ul style="list-style-type: none"><li>• 单个IP地址，如：192.168.10.5</li><li>• 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10</li><li>• 地址段，使用“/”隔开掩码，如：192.168.2.0/24</li></ul> <p><b>说明</b> 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。</p>	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”。	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”。	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”。	CN:中国大陆
域名	“目的地址类型”选择“域名”时，需填写“域名”。	www.example.com
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”。	域名组1
服务类型	选择 <b>服务或服务组</b> 。	服务
	<ul style="list-style-type: none"><li>• <b>服务</b>：支持设置单个服务。</li><li>• <b>服务组</b>：支持多个服务的集合。</li></ul>	

参数名称	参数说明	取值样例
协议/源端口/目的端口	设置需要限制的类型。 <ul style="list-style-type: none"><li>协议类型当前支持：TCP、UDP、ICMP、Any。</li><li>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</li><li>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，中间使用“-”隔开，如：80-443</li></ul>	TCP/443/443
服务组名称	自定义服务组名称。	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 6-8 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。	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
启用状态	选择该策略是否立即启用。 <ul style="list-style-type: none"><li>启用：表示启用，规则生效；</li><li>禁用：表示关闭，规则不生效。</li></ul>	启用
描述	自定义规则描述。	test
源地址类型	设置访问流量中发送数据的地址类型。 <ul style="list-style-type: none"><li><b>IP地址</b>：支持设置单个IP地址、连续多个IP地址、地址段。</li><li><b>IP地址组</b>：支持多个IP地址的集合。</li></ul>	IP地址

参数名称	参数说明	取值样例
源IP地址	<p>“源地址类型”选择“IP地址”时，需填写“源IP地址”。</p> <p>支持以下输入格式：</p> <ul style="list-style-type: none"><li>• 单个IP地址，如：192.168.10.5</li><li>• 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10</li><li>• 地址段，使用“/”隔开掩码，如：192.168.2.0/24</li></ul> <p><b>说明</b> 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。</p>	192.168.10.5
源地址组名称	<p>“源地址类型”选择“IP地址组”时，需填写“源地址组名称”。</p>	s_test
目的地址类型	<p>选择访问流量中的接收数据的地址类型。</p> <ul style="list-style-type: none"><li>• <b>IP地址</b>：支持设置单个IP地址、连续多个IP地址、地址段。</li><li>• <b>IP地址组</b>：支持多个IP地址的集合。</li></ul>	IP地址组
目的IP地址	<p>“目的地址类型”选择“IP地址”时，需填写“目的IP地址”。</p> <p>目的IP地址支持以下输入格式：</p> <ul style="list-style-type: none"><li>• 单个IP地址，如：192.168.10.5</li><li>• 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10</li><li>• 地址段，使用“/”隔开掩码，如：192.168.2.0/24</li></ul> <p><b>说明</b> 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。</p>	192.168.10.6
目的地址组名称	<p>“目的地址类型”选择“IP地址组”时，需填写“目的地址组名称”。</p>	d_test
服务类型	<p>选择<b>服务</b>或<b>服务组</b>。</p> <ul style="list-style-type: none"><li>• <b>服务</b>：支持设置单个服务。</li><li>• <b>服务组</b>：支持多个服务的集合。</li></ul>	服务



参数名称	参数说明	取值样例
协议/源端口/目的端口	设置需要限制的类型。 <ul style="list-style-type: none"><li>协议类型当前支持：TCP、UDP、ICMP、Any。</li><li>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</li><li>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，中间使用“-”隔开，如：80-443</li></ul>	TCP/443/443
服务组名称	自定义服务组名称。	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

## 6.5.2 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 CFW”，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


## 6.5.3 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 CFW”，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。

表 6-9 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。 <b>说明</b> 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。
规则类型	当前规则的防护类型，支持EIP规则和NAT规则。
方向	防护规则的流量方向。
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。
服务	<ul style="list-style-type: none"><li>协议类型当前支持：TCP、UDP、ICMP、Any。</li><li>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。</li><li>目的端口：当前开放或限制的端口号。支持单个端口，或者连续端口组，中间使用“-”隔开，如：80-443。</li></ul>
动作	<ul style="list-style-type: none"><li>“放行”：设置相应流量通过防火墙。</li><li>“阻断”：阻止相应流量通过防火墙。</li></ul>
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 <a href="#">访问控制日志</a> 。
启用状态	当前规则的启用状态，支持启用和禁用。
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 CFW”, 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 CFW”, 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

**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 CFW”, 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, 单击“确定”, 完成删除。

**警告**

删除规则后无法恢复，请谨慎操作。


----结束

## 6.5.4 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 CFW”，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** 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6-10](#)。

表 6-10 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”。 <ul style="list-style-type: none"><li>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。</li><li>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。</li></ul>
协议类型	协议类型当前支持：TCP、UDP、ICMP、Any。
端口	“协议类型”选择“TCP”或“UDP”时，设置需要放行或拦截的端口。 <b>说明</b> <ul style="list-style-type: none"><li>如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。</li><li>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”。</li><li>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”。</li></ul>
描述	设置该黑/白名单的备注信息。


参数名称	参数说明
IP地址列表	<ul style="list-style-type: none"><li>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。</li><li>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<a href="#">查看预定义地址组</a>。</li></ul> <p><b>注意</b> “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。</p>

**步骤6** 修改完成后，单击“确认”保存。

----结束

## 删除黑/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 CFW”，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** 在需要删除的规则所在行的“操作”列，单击“删除”。

**步骤6** 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。



**警告**

删除名单后无法恢复，请谨慎操作。

----结束

## 6.6 IP 地址组管理

### 6.6.1 添加自定义 IP 地址组和 IP 地址

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。


#### 约束条件

- 每个防火墙实例下最多添加3800个IP地址组。
- 每个IP地址组中最多添加640个IP地址成员。

- 每个防火墙实例下最多添加30000个IP地址。

## 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 CFW”，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，单击“添加IP地址组”，弹出“添加IP地址组”界面，填写参数如表 [添加IP地址组的参数说明](#)所示。

表 6-11 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。
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。
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： <ul style="list-style-type: none"><li>• 单个IP地址，如：192.168.10.5。</li><li>• 地址段，使用"/"隔开掩码，如：192.168.2.0/24。</li><li>• 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10。</li><li>• 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。</li></ul>

**步骤6** 确认无误后，单击“确认”，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 CFW”，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，单击添加的IP地址组名称，弹出“IP地址组详情”弹窗。

**步骤6** 单击“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。

**步骤7** 确认信息无误后，单击“确认”，完成添加IP地址。

----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”。

## 后续操作

IP地址组在防护规则里设置后才会生效，添加防护规则请参见[通过添加防护规则拦截/放行流量](#)。

## 6.6.2 查看预定义地址组

云防火墙为您提供预定义地址组，包括“NAT64转换地址组”和“WAF回源IP地址组”，两个地址组均建议您放行。

- NAT64转换地址组：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”。
- WAF回源IP地址组：提供Web应用防火墙（WAF）服务云模式的回源IP地址。

---


### 注意

- 引用至防护规则，如果回源IP改变，无需手动修改，防火墙每天自动更新地址组中的IP地址。
  - 添加至黑/白名单，如果回源IP改变，您需手动修改对应黑/白名单中的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。

## 查看预定义地址组

**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 CFW”，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，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，查看地址组信息。

----结束

## 6.6.3 删除自定义 IP 地址组


本文指导您删除自定义IP地址组。

### 约束条件

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。

### 删除自定义 IP 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 CFW”，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，在需要删除的IP地址组所在行的“操作”列，单击“删除”。

**步骤6** 在弹出的“删除IP地址组”界面，确认删除的信息无误后，输入“DELETE”，单击“确定”，完成删除。



删除IP地址组后无法恢复，请谨慎操作。

---

----结束

## 6.7 域名组管理

### 6.7.1 添加域名组

域名组是多个域名或泛域名的集合。您可以通过添加域名组批量对域名或泛域名进行防护。

提供以下两种类型：

- 应用域名组：支持**域名或泛域名**的防护；适用应用层协议，支持HTTP、HTTPS的应用协议类型；通过域名匹配。
- 网络域名组：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。



## 匹配策略

- 应用域名组：CFW会将会话中的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。
- 网络域名组：CFW会在后台获取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。  
单个域名最大支持解析1000条IP地址；每个域名组最大支持解析1500条IP地址。解析结果达到上限，则无法再将新域名添加到域名组中

### 📖 说明

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。

## 约束条件

- 域名组成员不支持添加中文域名格式。
- 域名组中所有域名被“防护规则”引用最多40000次，泛域名被“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。

### 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。

## 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 CFW”，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** （可选）如果添加网络域名组，则选择“网络域名组”页签。

**步骤6** 切换至“域名组”页签，单击“添加域名组”，弹出“添加域名组”，填写参数如[表 添加域名组参数说明](#)所示。

表 6-12 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

参数名称	参数说明
域名组名称	自定义域名组名称。
描述	(可选) 设置该域名组的备注信息。
域名	输入域名, 规则如下: <ul style="list-style-type: none"><li>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)。</li><li>多个域名以英文逗号、英文分号、换行符、空格分隔。</li></ul> <b>说明</b> 输入的域名请勿重复。

----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 CFW”, 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, 单击添加的域名组名称。弹出“域名组”弹窗。

**步骤6** 单击“添加域名”, 弹出“添加域名”对话框, 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

## 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”界面, 批量勾选域名后, 单击列表上方的“删除”。
- 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[通过添加防护规则拦截/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”。


## 6.7.2 删除域名组

### 约束条件

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。

### 删除域名组

**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 CFW”，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** （可选）如删除网络域名组，则选择“网络域名组”页签。

**步骤6** 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。



**警告**

删除域名组后无法恢复，请谨慎操作。

----结束

## 6.8 服务组管理

### 6.8.1 添加自定义服务组和服务


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。

### 约束条件

- 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。

### 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 CFW”，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“服务组”页签，单击“添加服务组”，弹出“添加服务组”界面，填写服务组名称及描述。

表 6-13 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。
服务列表	<ul style="list-style-type: none"><li>● 协议：当前支持的协议为：TCP、UDP、ICMP。</li><li>● 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</li><li>● 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</li><li>● 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。</li></ul>

**步骤6** 确认填写信息无误后，单击“确认”，完成添加服务组。

----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 CFW”，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“服务组”页签，单击添加的服务组名称。弹出“服务组”弹窗。

**步骤6** 单击“添加服务”，弹出“添加服务”对话框。

表 6-14 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 <b>说明</b> 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  <b>说明</b> 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** 单击添加可添加多个服务。

**步骤8** 确认无误后，单击“确认”，完成添加。

----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”界面，批量勾选服务后，单击列表上方的“删除”。

## 后续操作

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[通过添加防护规则拦截/放行流量](#)。


## 6.8.2 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。

预定义服务组仅支持查看，不支持添加、修改、删除操作。

### 查看预定义服务组

**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 CFW”，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“服务组”页签，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

### 6.8.3 删除自定义服务组

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。


本文指导您删除自定义服务组。

#### 约束条件

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。

#### 删除自定义服务组

**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 CFW”，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“服务组”页签，在待删除的服务组所在行的“操作”列，单击“删除”。

**步骤6** 在弹出的“删除服务组”界面，确认删除的信息无误后，输入“DELETE”，单击“确定”，完成删除。



删除服务组后无法恢复，请谨慎操作。

---

----结束

# 7 拦截恶意攻击

## 7.1 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[开启互联网边界流量防护](#)。
- 开启VPC流量防护请参见[开启VPC边界流量防护](#)。

### 如何防御网络攻击和病毒文件

提供以下几种方式：

- 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，覆盖多种常见的网络攻击，有效保护您的资产。
  - IPS提供四种防护模式，如需调整防护模式请参见[调整IPS防护模式拦截网络攻击](#)。
    - **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。
    - **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。
  - IPS提供多类规则库，详细介绍如[表7-1](#)所示，不同防护模式会开启不同规则的“拦截”状态，对照表请参见[规则组随防护模式变更的默认动作对照表](#)。

表 7-1 入侵防御规则库介绍

功能名称	功能描述	检测类型	配置方式
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。	<ul style="list-style-type: none"><li>检查威胁及漏洞扫描；</li><li>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；</li><li>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。</li></ul>	查看和修改规则库请参见 <a href="#">修改入侵防御规则的防护动作</a>
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）	提供的规则库无法满足需求时，支持自定义特征规则。	检测类型和“基础防御”一致。  支持添加HTTP、TCP、UDP、POP3、SMTP、FTP协议类型的特征规则。	请参见 <a href="#">自定义IPS特征</a>

- 敏感目录扫描防御：防御对云主机敏感目录的扫描攻击，配置方式请参见[开启敏感目录扫描防御](#)。
- 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，配置方式请参见[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。  
病毒防御功能请参见[拦截病毒文件](#)。

## 防护动作介绍

- 观察：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：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：防火墙对匹配当前规则的流量，不记录、不拦截。



## 相关文档

详细日志信息请参见[攻击事件日志](#)。

## 7.2 拦截网络攻击


云防火墙提供[网络攻击防护](#)，帮助您检测常见的网络攻击。

### 对业务的影响

调整防护模式时，建议您优先开启“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”。

### 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 CFW”，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** 选择合适的防护模式。

- **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。
- **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[IPS规则管理](#)。

----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 CFW”，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“高级”，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，拦截当次会议。
  - 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”。

----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 CFW”，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“高级”，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，拦截当次会议。
  - 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，确保攻击能够及时发现并处理。

----结束

## 后续操作

详细日志信息请参见[攻击事件日志](#)。

## 7.3 拦截病毒文件

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。


病毒防御功能支持检测HTTP、SMTP、POP3、FTP、IMAP4、SMB的协议类型。

### 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 CFW”，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。


#### 说明

开启病毒防御功能后，防火墙“当前动作”默认为“禁用”，修改防御动作请参见[修改病毒防御动作提升防护效果](#)。

----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 CFW”，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“防御规则”列表中“操作”列的按钮，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

详细日志信息请参见[攻击事件日志](#)。

## 7.4 IPS 规则管理

### 7.4.1 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，该规则不受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[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：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：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：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

**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 CFW”，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“基础防御”中的“查看生效中的规则”，进入“基础防御规则”页面。

**步骤6** （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7** 单击待修改动作的“操作”列，选择对应动作。

- 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。

### 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

## 相关操作

- 恢复部分规则的默认动作：“基础防御规则”页面，勾选规则，单击上方“恢复默认”。
- 恢复全部规则的默认动作：“基础防御规则”页面，单击上方“全局恢复默认”。

## 7.4.2 自定义 IPS 特征

CFW支持自定义网络入侵特征规则，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。

### 注意


自定义的特征建议具体化，避免太宽泛，否则可能会导致大部分流量匹配到该特征规则，影响流量转发性能。

## 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”。

## 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 CFW”，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”。单击“自定义IPS特征”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，单击列表右上角“添加自定义IPS特征”，填写规则如表 [添加自定义IPS特征](#) 所示。

表 7-2 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。
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。 <ul style="list-style-type: none"><li>• 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。</li><li>• 服务器到客户端</li><li>• 客户端到服务器</li></ul>
协议类型	选择特征的协议类型。
源类型	选择源端口类型。 <ul style="list-style-type: none"><li>• Any: 任意端口类型，等同于包含所有类型。</li><li>• 包含</li><li>• 排除</li></ul> <p><b>说明</b> 建议您优先选择“Any”。</p>

参数名称	参数说明
源端口	<p>“源类型”选择“包含”或“排除”时，设置源端口。</p> <ul style="list-style-type: none"><li>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。</li><li>支持连续端口组，中间使用“-”隔开，如：80-443。</li></ul>
目的类型	<p>选择目的端口类型。</p> <ul style="list-style-type: none"><li>Any：任意端口类型，等同于包含所有类型。</li><li>包含</li><li>排除</li></ul> <p><b>说明</b> 建议您优先选择“Any”。</p>
目的端口	<p>“目的类型”选择“包含”或“排除”时，设置目的端口。</p> <ul style="list-style-type: none"><li>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。</li><li>支持连续端口组，中间使用“-”隔开，如：80-443。</li></ul>
动作	<p>防火墙检测到该特征流量时，采取的动作。</p> <ul style="list-style-type: none"><li>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<a href="#">日志查询</a>。</li><li>拦截：实施自动拦截操作。</li></ul> <p><b>说明</b> 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”。</p>

参数名称	参数说明
内容	<p>特征规则中匹配的内容。</p> <ul style="list-style-type: none"><li>内容：跟特征匹配的内容字段，例如：cfw。</li><li>内容选项：选择“内容”匹配的限制规则。<ul style="list-style-type: none"><li>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。</li><li>忽略大小写：匹配时不区分大小写。</li><li>URL：匹配URL中跟“内容”一致的字段。</li></ul></li><li>相对位置：匹配特征时，指定开始的位置。<ul style="list-style-type: none"><li>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。<p><b>说明</b></p>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。</li><li>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。</li></ul></li><li>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。</li><li>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。<p><b>说明</b></p><ul style="list-style-type: none"><li>“深度”值需大于“内容”字段长度。</li><li>一条IPS特征中最多添加4条内容。</li></ul></li></ul>

**步骤6** 单击“确认”，完成添加IPS特征。

----结束

## 相关操作

- 复制IPS特征：在目标任务所在行的“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IPS特征：在目标任务所在行的“操作”列中，单击“编辑”，可以修改IPS特征信息。
- 批量删除IPS特征：勾选目标特征，单击列表上方的“删除”，可以批量删除IPS特征。
- 批量修改动作：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。



## 后续操作

详细日志信息请参见[攻击事件日志](#)。

# 8 查看流量数据

## 8.1 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[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 CFW”，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。

表 8-1 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

- 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8-2。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 8-2 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。
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

## 8.2 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[开启互联网边界流量防护](#)。

### 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 CFW”，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。

表 8-3 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

- 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8-4。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 8-4 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。
TOP访问目的地区	出方向流量的目的IP所属的地理位置。
TOP访问域名	出方向流量的域名信息。
TOP访问源IP	出方向流量的源IP地址。
TOP开放端口	出方向流量的目的端口。
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。

----结束

## 8.3 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[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 CFW”，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。

**表 8-5** 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

- 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8-6。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 8-6** 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

# 9 查看云防火墙防护日志

## 9.1 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，出现误拦截时您可以修改防护动作，操作步骤请参见[修改入侵防御规则的防护动作](#)，修改病毒防御的防护动作请参见[修改病毒防御动作提升防护效果](#)。
- 访问控制日志：命中访问控制策略的所有流量，修改防护规则请参见[管理防护规则](#)，修改黑白名单请参见[编辑黑/白名单](#)。
- 流量日志：查看通过防火墙的所有流量记录。

### 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1000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 CFW”，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，可查看近一周的攻击事件详情。

表 9-1 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。

参数	说明
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。
标签	IP类型标识。 <ul style="list-style-type: none"><li>其它标签：非WAF回源IP，无需特别处理。</li><li>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”。</li></ul>
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。 <ul style="list-style-type: none"><li>放行</li><li>阻断</li><li>阻断IP</li><li>丢弃</li></ul>
操作	操作：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 CFW”，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“访问控制日志”页签，可查看近一周的访问控制流量详情。如果需要修改指定IP访问控制的响应动作，请参照[通过添加防护规则拦截/放行流量](#)或[通过添加黑白名单拦截/放行流量](#)。


表 9-2 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 CFW”，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。

表 9-3 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。



参数	说明
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

## 相关操作

导出日志：单击右上角的，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。
- 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](#)。

# 10 系统管理

## 10.1 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 CFW”，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”，设置通知项参数，参数说明如表 [攻击告警参数说明](#)所示。

表 10-1 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。
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。

参数名称	参数说明
通知时间	选择通知的时间段。
触发条件	设置触发条件。 <b>说明</b> 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 CFW”，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”，设置通知项参数，参数说明如表 [流量超额预警参数说明](#) 所示。

表 10-2 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（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。
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 CFW”，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”，设置通知项参数，参数说明如表 [EIP未防护告警参数说明](#) 所示。

表 10-3 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。
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

## 相关操作

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。

## 10.2 DNS 服务器配置

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。

## 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 CFW”，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** 单击“应用”，完成配置。

### 说明

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

## 10.3 安全报告管理

### 10.3.1 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 CFW”，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”创建报告模板，参数说明如表 [创建报告模板参数说明](#) 所示。

表 10-4 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	<ul style="list-style-type: none"><li>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。</li><li>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。</li><li>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。</li></ul>
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。 <b>说明</b> 为了保证正确性，报告发送时间可能存在延迟。
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

## 10.3.2 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 CFW”，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，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 CFW”，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，单击右下角的“下载”，可获取报告。


----结束

## 10.3.3 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。

### 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 CFW”，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 CFW”，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 10-5** 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	<ul style="list-style-type: none"><li>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。</li><li>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。</li></ul>
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。
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 CFW”，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



# 11 常见问题

## 11.1 产品咨询

### 11.1.1 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。

### 11.1.2 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。

### 11.1.3 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VPC边界、Web服务提供防护。

WAF和CFW的主要区别说明如[表11-1](#)所示。

表 11-1 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。

类别	云防火墙	Web应用防火墙
防护对象	<ul style="list-style-type: none"> <li>弹性公网IP和VPC边界。</li> <li>支持对Web攻击的基础防护。</li> <li>支持外部入侵和主动外联的流量防护。</li> </ul>	<ul style="list-style-type: none"> <li>针对域名或IP，云上或云下的Web业务。</li> <li>支持对Web攻击的全面防护。</li> </ul>
功能特性	<ul style="list-style-type: none"> <li>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。</li> <li>访问控制：支持互联网边界访问流量的访问控制。</li> <li>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。</li> </ul>	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。

### 11.1.4 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11-2所示。

表 11-2 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
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。

类别	云防火墙	安全组	网络ACL
防护场景	<ul style="list-style-type: none"><li>• 互联网边界</li><li>• VPC边界</li><li>• SNAT场景</li></ul>	弹性云服务器	子网
功能特性	<ul style="list-style-type: none"><li>• 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。</li><li>• 支持通过地理位置、域名、域名组、黑/白名单过滤。</li><li>• 支持入侵防御系统（IPS）、病毒防御（AV）功能。</li></ul>	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。

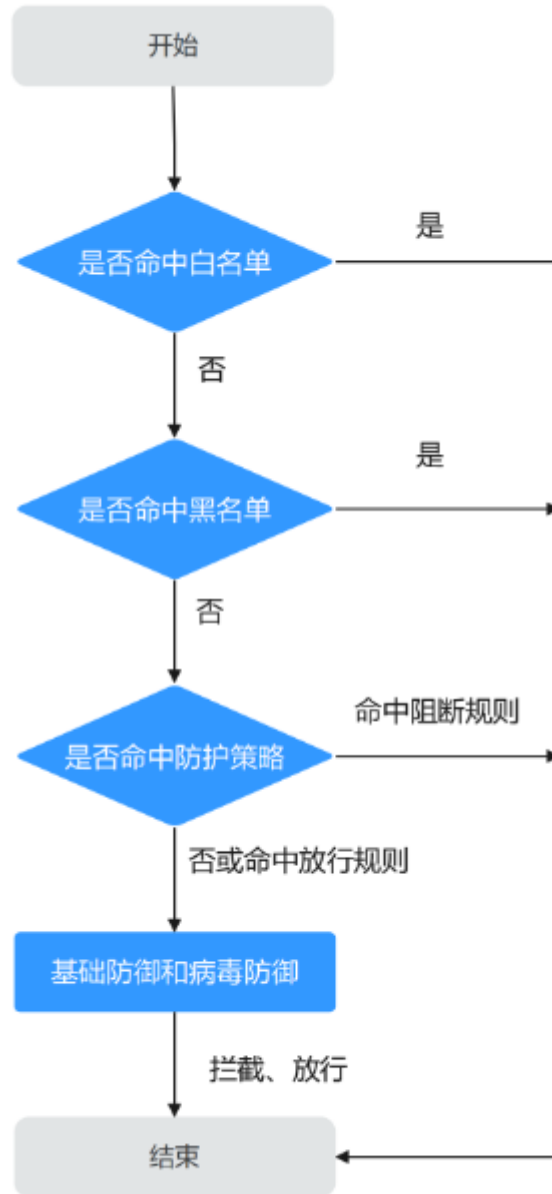
### 11.1.5 云防火墙支持哪些维度的访问控制？

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。

### 11.1.6 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 11-1 防护顺序



- 设置黑/白名单请参见[管理黑白名单](#)。
- 添加防护规则请参见[通过添加防护规则拦截/放行流量](#)。
- 设置IPS防护模式请参见[拦截网络攻击](#)。
- 开启病毒防御请参见[拦截病毒文件](#)。

### 11.1.7 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

## 11.2 故障排查

### 11.2.1 业务流量异常怎么办？

当您的业务流量异常，可能被CFW中断时，可按照本节内容排查故障。

#### 问题描述

业务流量异常，例如：

- EIP无法访问公网
- 无法访问某个服务器

#### 排查思路

图 11-2 业务流量异常排查思路

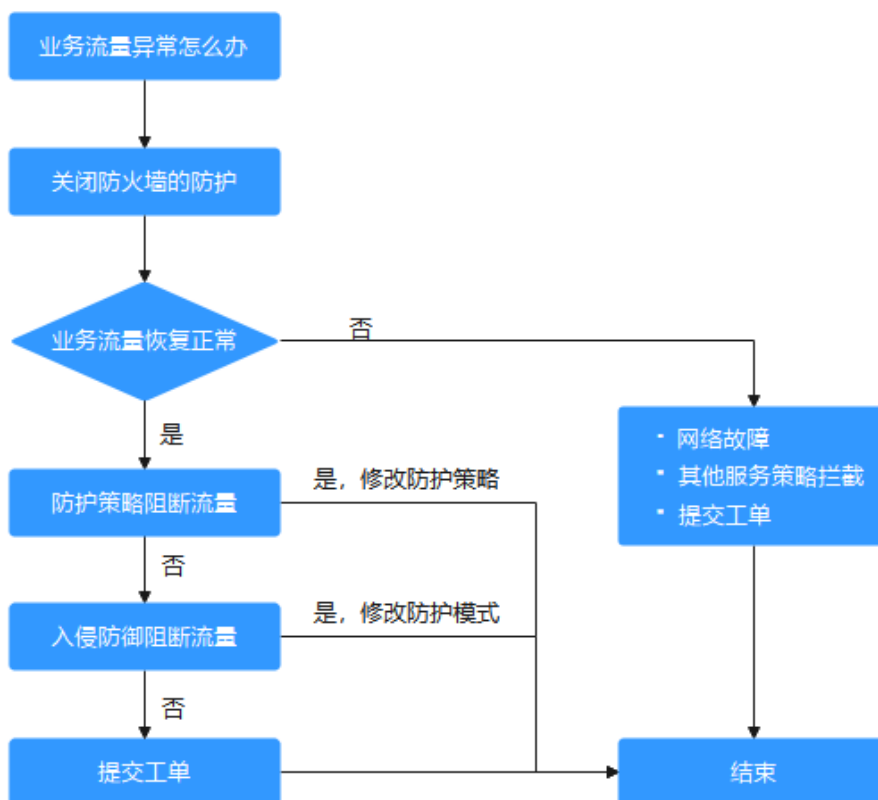


表 11-3 业务流量异常排查思路

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 <a href="#">原因一：非CFW造成的流量中断</a>
2	防护策略阻断流量	解决方法请参考 <a href="#">原因二：防护策略阻断流量</a>
3	入侵防御阻断流量	解决方法请参考 <a href="#">原因三：入侵防御阻断流量</a>

## 原因一：非 CFW 造成的流量中断

可以在云防火墙控制台，关闭防护，观察业务情况，如果业务仍未恢复，说明非CFW造成的流量中断。

关闭防护的方式如下：

- 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[开启/关闭VPC边界防火墙（虚拟私有云）](#)。

如果业务仍未恢复，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。

## 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

- 若无记录，请参见[表11-3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：
    - 删除该条黑名单策略。
    - 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：
    - 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。
    - 修改对应的阻断策略的匹配条件，移除该IP/域名信息。

- 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[通过添加防护规则拦截/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，防火墙管理员登录云防火墙控制台，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 11-3 弹性公网 IP 列表

弹性公网IP ID	防护状态	弹性公网ID	企业项目	已绑定实例	标签	操作
126a098e-4300-4582-996a-be371c109e06	防护中	CFW-backup 2e7f82d4-0a69-4fb5-a7d9-fa6c112d43b7		efs-efs08 云服务器	--	关闭防护
a9f8927-dc4e-4ee3-b58b-cf83194d7950	防护中	CFW-backup 2e7f82d4-0a69-4fb5-a7d9-fa6c112d43b7	CFW_test	ecs-cfw-test2 云服务器	combined_order_id=CBRCIS...	关闭防护
b059061-798c-49a2-57ab-2984e4343d82	防护中	CFW-backup 2e7f82d4-0a69-4fb5-a7d9-fa6c112d43b7	CFW_test	ecs-cfw-test1 云服务器	combined_order_id=CBRCIS...	关闭防护
126 8e529116-4e6e-46c8-83ee-87b2655098d8	防护中	CFW-backup 2e7f82d4-0a69-4fb5-a7d9-fa6c112d43b7		ecs-sec-tools 云服务器	--	关闭防护

**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 11-4 筛选访问控制日志

访问时间	访问源	源IP地址	源端口	访问目的IP	目的IP地址	目的端口	协议	响应动作	规则
2023/12/22 02:20:42 G...	126	Chinese Mainland	40005		Chinese Mainland	123	UDP	阻断	阻断违规外联
2023/12/22 02:46:23 G...	126	Chinese Mainland	46887		Chinese Mainland	123	UDP	阻断	阻断违规外联
2023/12/22 02:46:13 G...	126	Chinese Mainland	51444		Chinese Mainland	123	UDP	阻断	阻断违规外联
2023/12/22 02:46:03 G...	126	Chinese Mainland	39664		Chinese Mainland	123	UDP	阻断	阻断违规外联
2023/12/22 02:45:53 G...	126	Chinese Mainland	48842		Sweden	123	UDP	阻断	阻断违规外联
2023/12/22 02:45:42 G...	126	Chinese Mainland	59171		Hong Kong (China)	123	UDP	阻断	阻断违规外联

**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 11-5 搜索防护规则

优先级	名称	方向	源	目的	服务	动作	命中次数	启用状态	标签	操作
1	禁止访问	内-外	126	*.*.*.*.com	TCP:1-65535:1-65535	阻断	0	开启	--	编辑 设置优先级 更多
3	阻断违规外联	内-外	0.0.0.0/0	0.0.0.0/0	Any	阻断	9,821	开启	98%Hit	编辑 设置优先级 更多
4	阻断访问外网流量	内-外	126	南美洲、欧洲、非洲、北...	Any	阻断	0	开启	--	编辑 设置优先级 更多

**注意**

**图 搜索防护规则**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 搜索防护规则**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，在云防火墙控制台“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。

- 若无记录，请排查问题。
- 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**拦截网络攻击**。
  - 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**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：

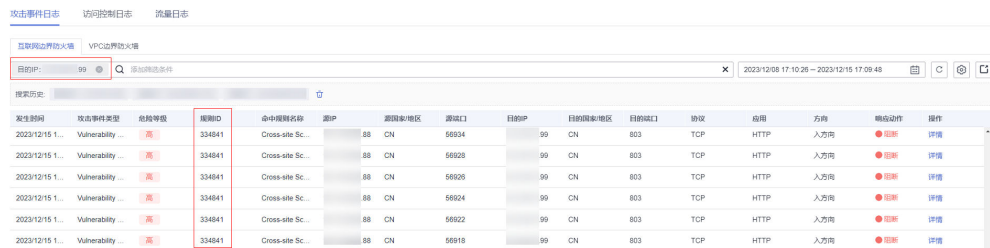
**步骤1** 为优先保证业务恢复，防火墙管理员登录云防火墙控制台，进入“攻击防御 > 入侵防御”，将“防护模式”由“严格模式-拦截”改为“观察模式”。

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 11-6 筛选攻击事件日志



**步骤3** 通过查看“详情 > 攻击payload”和抓包，确认该业务为正常业务。于是管理员参考了[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 11-7 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

## 提交工单

如果上述方法均不能解决您的疑问，请寻求更多帮助。

## 11.2.2 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。


## 11.2.3 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 CFW”，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，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。
- 方向：外-内
  - 源：Any
  - 目的：Any
  - 服务：Any
  - 应用：Any
  - 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6** 配置放行规则。添加防护规则请参见[通过添加防护规则拦截/放行流量](#)。
- 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[调整防护规则的优先级](#)。
- 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[开启互联网边界流量防护](#)。

## 11.2.4 IPS 拦截了正常业务如何处理？

如果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[拦截网络攻击](#)。

### 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 CFW”，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 11-8 规则 ID

攻击事件类型	危险等级	规则ID	命中规则名称
Vulnerability ...	高	336842	Simple HTT...

**步骤5** 单击“基础防御”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

## 11.2.5 为什么访问控制日志页面数据为空？

访问控制日志展示的是ACL防护策略匹配到的流量，您需要配置ACL策略才能查看访问控制日志。

- 添加防护规则请参见[通过添加防护规则拦截/放行流量](#)。
- 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](#)。

## 11.3 网络流量

### 11.3.1 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（入流量）和业务主动外联访问的流量（出流量）。

### 11.3.2 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。

### 11.3.3 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 进入云防火墙管理控制台，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，若无新增，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

# A 修订记录

发布日期	修改说明
2024-12-03	第一次正式发布。