云防火墙

用户指南

文档版本 17

发布日期 2025-01-22

华为云计算技术有限公司

商标声明


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。

目 录

1 创建用户组并授权使用 CFW

如果您需要对您所拥有的CFW进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织架构，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用CFW资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将CFW资源委托给更专业、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

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

本章节为您介绍对用户授权的方法，操作流程如**图1-1**所示。

前提条件

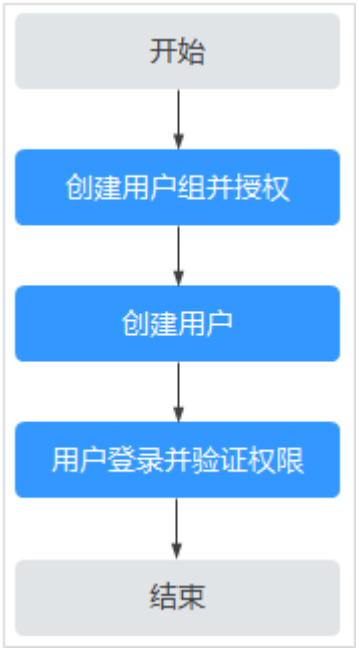
给用户组授权之前，请您了解用户组可以添加的CFW权限，并结合实际需求进行选择，CFW支持的系统权限如**表1-1**所示。

表 1-1 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
CFW ReadOnlyAccess	云防火墙服务的只读权限。	系统策略	无

示例流程

图 1-1 给用户授权服务权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予CFW只读权限“CFW ReadOnlyAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，切换至授权区域，验证权限：
   - 在“服务列表”中选择云防火墙，进入CFW主界面，单击“购买云防火墙”，尝试购买云防火墙，如果无法购买云防火墙（假设当前权限仅包含CFW ReadOnlyAccess），表示“CFW ReadOnlyAccess”已生效。
   - 在“服务列表”中选择除CFW外（假设当前策略仅包含“CFW ReadOnlyAccess”）的任一服务，若提示权限不足，表示“CFW ReadOnlyAccess”已生效。

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、流量拓扑可视化信息，随时了解云资产的安全状况以及流量数据。

约束条件

VPC边界防护详情需配置**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**。

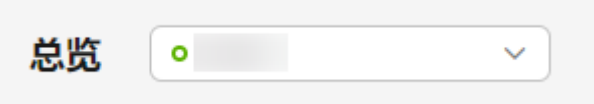
步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （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。

  图 2-1 切换防火墙实例

- 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**。

  图 2-2 查看防火墙实例信息

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

步骤5 在“资源概况”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6 在“安全事件”中，查看入侵防御功能的防护总详情，快速定位需要防护的云资产。

- 在右上角切换查询时间，支持查询5分钟~7天的数据。
- 为异常外联的IP地址添加防护策略：
  a. 单击“异常外联IP数”的数字。
  b. 在弹框中选择需要防护的IP地址。
  c. 生成地址组：
     - 创建为地址组：生成新的地址组。
     - 添加到地址组：添加到已有的地址组。
  d. 将地址组添加到防护规则或黑/白名单，请参见**访问控制策略概述**。

步骤7 在“防护规则”中，查看防护策略的未命中数量和总数。

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

步骤8 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 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。

参数名称		参数说明
	防火墙ID	当前防火墙实例的ID。
	状态	当前防火墙的状态。开通或退订防火墙大约需要5分钟更新状态。
	企业项目	当前防火墙所属的企业项目。
规格	已使用/可防护EIP数	当前防火墙实例已开启防护的弹性公网IP数量/可防护的弹性公网IP总数。
	已使用/可防护VPC数	当前防火墙实例已开启防护的VPC数量/可防护的VPC总数。
	互联网边界防护带宽	所有经过云防火墙防护的EIP的流量总和最大值，按照入云流量（入流量）或出云流量（出流量）的最大值取值。
	VPC边界防护带宽	可防护的东西向流量峰值。 所有经过云防火墙防护的VPC的流量总和最大值。
	已使用/可使用防护规则	当前防火墙实例已创建的防护规则数量/可创建的防护规则总数。
交易信息	计费模式	购买的计费模式。
	到期处理策略	到期后的费用策略。
	创建时间	防火墙实例的创建时间。
	到期时间	防火墙实例的预计到期时间
	最近交易订单	防火墙实例最新的交易订单。
标签		用于标识防火墙，方便您对防火墙进行分类和跟踪。 关于标签管理服务TMS，请参见**资源标签简介**。

步骤9 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，支持查询5分钟~7天的数据。

- 查看访问控制策略的拦截效果，以及出/入方向流量的95带宽和最大值。
  - 流量峰值：系统每个周期统计1个带宽值，某段时间内统计的最大值即流量峰值。

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

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

说明

周期取值说明：

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

- 流量趋势：查看出/入方向和整体的流量变化趋势，可在右上角选择“平均值”或“最大值”。

表 2-3 取值说明

时间段	平均值	最大值
近1小时	取1分钟内的平均值	取1分钟内的最大值
近24小时	取5分钟内的平均值	取5分钟内的最大值
近7天	取1小时内的平均值	取1小时内的最大值
自定义	- 5分钟~6小时：取1分钟内的平均值 - 6小时（含）~3天：取5分钟内的平均值 - 3天（含）~7天（含）：取30分钟内的平均值	- 5分钟~6小时：取1分钟内的最大值 - 6小时（含）~3天：取5分钟内的最大值 - 3天（含）~7天（含）：取30分钟内的最大值

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 购买及变更云防火墙

3.1 购买包年/包月云防火墙

包年/包月计费模式是一种预付费方式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。

云防火墙支持一个区域下购买多个防火墙，便于管理不同场景下的资源和策略。

前提条件

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

约束条件

- 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**功能总览**。

版本信息说明

云防火墙支持包年/包月（预付费）和按需计费两种计费方式。

- 包周期（包年/包月）提供以下服务版本：标准版、专业版；
- 按需计费提供专业版防火墙。

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。

购买云防火墙

根据您需要的防火墙实例版本，参考以下操作购买。

标准版防火墙

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 单击“购买云防火墙”，进入“购买云防火墙”页面，相关参数如表3-1所示。

表 3-1 购买标准版防火墙参数说明

参数名称		参数说明
计费模式		选择“包年/包月”，按配置周期计费。
区域		购买云防火墙的区域。 **须知** 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**云防火墙支持哪些区域？**。
版本规格	-	选择版本：标准版。
	扩展防护公网IP数	（可选）选择需扩展的防护公网IP数，可选择范围：0~2000个 **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。
	扩展互联网边界防护带宽	（可选）选择需扩展的防护流量峰值（出流量或入流量的最大峰值），可选择范围：0~50,000Mbps/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（套餐内费用包含），如果您的防护流量是200Mbps，那么只需要填写190Mbps。 • 防护流量按照出流量或入流量的最大峰值取值。
高级设置	防火墙名称	设置当前防火墙的名称。 命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）、空格和特殊字符（-_）。 • 长度支持1-48个字符。

参数名称		参数说明
	企业项目	在下拉列表中选择您所在的企业项目，选择后，云防火墙将归属到该项目下，云防火墙支持防护当前账号所有企业项目下的资源。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。
	标签	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，请参见**资源标签简介**。 如您的组织已经设定云防火墙的相关标签策略，则需按照标签策略规则为防火墙实例添加标签。标签如果不符合标签策略的规则，则可能会导致防火墙创建失败，请联系组织管理员了解标签策略详情。
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。自动续费规则请参见**自动续费规则说明**。

步骤5 确认信息无误后，单击“立即购买”。

步骤6 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

专业版防火墙

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的  ，选择区域。

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

步骤4 单击“购买云防火墙”，进入“购买云防火墙”页面，相关参数如**表 购买包年/包月云防火墙的参数说明**所示。

表 3-2 购买专业版防火墙参数说明

参数名称		参数说明
基础配置	计费模式	选择“包年/包月”，按配置周期计费。
	区域	购买云防火墙的区域。 **须知** 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**云防火墙支持哪些区域?** 。
版本规格	-	选择版本：专业版。
	扩展防护公网IP数	（可选）选择需扩展的防护公网IP数，可选择范围：0~2,000个 **说明** 此处为套餐外购买数量，例如专业版防护公网IP数默认50个（套餐内费用包含），如果您的公网IP是65个，那么只需要填写15个。
	扩展互联网边界防护带宽	（可选）选择需扩展的防护流量峰值（出流量或入流量的最大峰值），可选择范围：0~50,000Mbps/月（需为5的整数倍） **说明** • 此处为套餐外购买流量值，例如专业版防护互联网边界流量峰值默认50Mbps（套餐内费用包含），如果您的防护流量是200Mbps，那么只需要填写150Mbps。 • 防护流量按照出流量或入流量的最大峰值取值。
	扩展防护VPC数	（可选）选择需扩展的VPC数，可选择范围：0~1,000个。 **说明** • 仅“专业版”支持VPC间防护功能， • 此处为套餐外购买数量，例如专业版防护VPC数默认2个（套餐内费用包含），如果您的VPC是3个，那么只需要填写1个。 • “扩展VPC数”每增加1个，“扩展VPC间防护流量峰值”增加200Mbps。
高级设置	企业项目	在下拉列表中选择您所在的企业项目，选择后，云防火墙将归属到该项目下，云防火墙支持防护当前账号所有企业项目下的资源。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。

参数名称		参数说明
	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。
	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，请参见**资源标签简介**。 如您的组织已经设定云防火墙的相关标签策略，则需按照标签策略规则为防火墙实例添加标签。标签如果不符合标签策略的规则，则可能会导致防火墙创建失败，请联系组织管理员了解标签策略详情。
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。自动续费规则请参见**自动续费规则说明**。

步骤5 确认信息无误后，单击“立即购买”。

步骤6 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

3.2 购买按需计费云防火墙

按需付费是后付费方式，可以随时开通/删除云防火墙，支持秒级计费，系统会根据防护流量的实际情况每小时出账单，并从账户余额里扣款。

云防火墙支持一个区域下购买多个防火墙，便于管理不同场景下的资源和策略。

前提条件

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

约束条件

- 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**功能总览**。
- 最大支持防护1 Gbps带宽流量（经过防火墙的总流量）。
- 仅专业版支持按需计费购买。

购买按需计费专业版防火墙

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 单击“购买云防火墙”，进入“购买云防火墙”页面，相关参数如表 购买按需计费云防火墙参数说明所示。

表 3-3 云防火墙参数说明

参数名称	参数说明
计费模式	选择“按需计费”，从购买开始到退订结束，按实际防护情况计费。
区域	购买云防火墙的区域。 **须知** 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**云防火墙支持哪些区域？**。
版本规格	目前仅支持“专业版”。
防火墙名称	设置当前防火墙的名称。 命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）、空格和特殊字符（-_）。 • 长度支持1-48个字符。
企业项目	在下拉列表中选择您所在的企业项目，选择后，云防火墙将归属到该项目下，云防火墙支持防护当前账号所有企业项目下的资源。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。
标签	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。

步骤5 确认信息无误后，单击“立即购买”。

步骤6 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

3.3 升级云防火墙版本

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

约束限制

仅包周期（包年/包月）防火墙支持升级服务版本，“按需计费”购买的防火墙仅支持专业版且按照实际防护流量计费，无需变更防火墙规格。

从标准版升级到专业版

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在页面左上角，单击“升级到专业版”，进入“购买云防火墙”页面。

步骤6 确认版本规格后，单击“立即购买”。

步骤7 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。

步骤8 在“付款”页面，选择付款方式进行付款。

----结束

相关操作

- 如何为云防火墙续费?
- 如何退订云防火墙?

3.4 变更云防火墙扩展包数量

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

约束限制

- 仅包周期（包年/包月）防火墙支持变更扩展包数量。
- 互联网边界流量峰值标准版最大支持扩展到5G，专业版最大支持扩展到10G。

变更扩展包

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

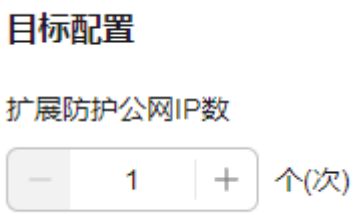
步骤3 在左侧导航栏中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

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

步骤5 变更扩展包数量。

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

图 3-1 扩展 EIP 防护数量



步骤6 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。

步骤7 在“付款”页面，选择付款方式进行付款。

----结束

退订扩展包

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在“防火墙详情”模块右侧，单击“退订”。

图 3-2 退订

步骤6 选择退订的扩展包，单击“确认”。

步骤7 确认信息无误后，勾选“我已确认本次退订金额和相关费用。”

步骤8 单击“下一步”，完成退订操作。

----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。

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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 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。

步骤7 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。
- 导出弹性公网IP列表信息：在列表上方，单击“导出”，根据数据范围选择选项。
- 如果需要防护其他账号下的EIP，请参见**多账号防护**。

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。

支持的防护对象

- 虚拟私有云（VPC）
- 虚拟网关（VGW）
- VPN网关（VPN）
- 企业连接网（ECN）
- 全球接入网关（DGW）

约束条件

- 仅“专业版”支持VPC边界防火墙。
- 依赖企业路由器（Enterprise Router, ER）服务引流。
- 仅支持防护当前账号企业项目下的VPC。
- 如果您存在私用公网(即使用10.0.0.0/8、 172.16.0.0/12、192.168.0.0/16 以及运营商级NAT保留网段100.64.0.0/10 以外的公网网段作为私网地址段)的情况，请您**提交工单**进行私网网段扩容，否则云防火墙可能无法正常转发您VPC间的流量。

配置及使用流程

VPC边界防火墙企业路由器模式因版本依赖，在不同局点上有着“新版”和“旧版”两个版本。

- 新版VPC边界防火墙：配置流程请参见**表 企业路由器模式（新版）配置及使用流程**，配置文档请参见**企业路由器模式（新版）**。

图 5-1 VPC 边界防火墙（新版）

- 旧版VPC边界防火墙：配置流程请参见**图 企业路由器关联模式配置流程**，配置文档请参见**企业路由器模式（旧版）**。

图 5-2 创建 VPC 边界防火墙（旧版）

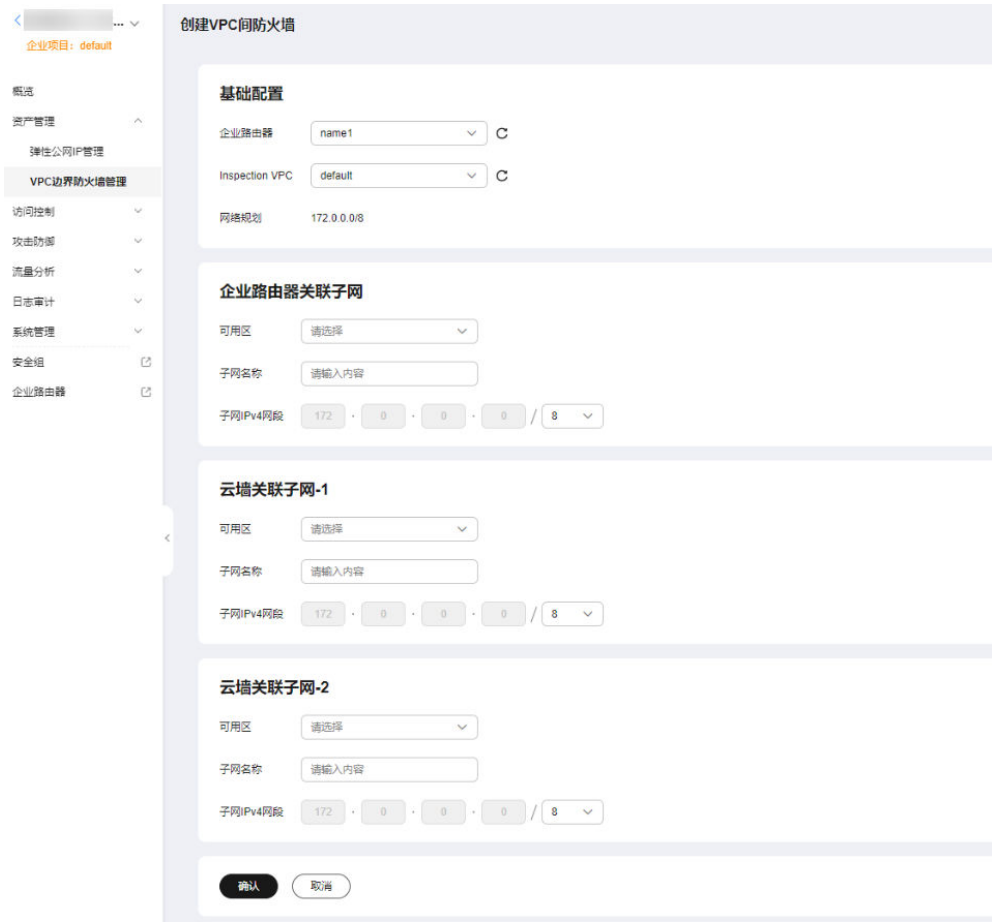
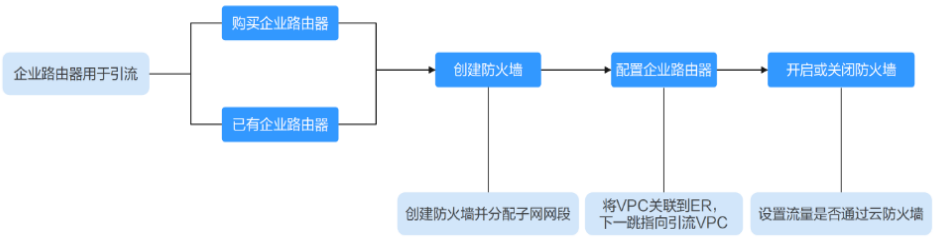


表 5-1 企业路由器模式（新版）配置及使用流程

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

下图为企业路由器模式（旧版）的配置流程：

图 5-3 企业路由器模式配置流程



5.2 企业路由器模式（新版）

5.2.1 创建 VPC 边界防火墙

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

前提条件

当前账号下需存在可用的企业路由器（企业路由器限制）。

- 关于企业路由器的收费，请参见**企业路由器计费说明**。
- 创建企业路由器请参见**创建企业路由器**。

  说明

  创建时，建议取消勾选“默认路由表关联”和“默认路由表传播”。

创建说明

创建防火墙时为了引流需选择企业路由器和配置IPV4网段。

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

创建 VPC 边界防火墙

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

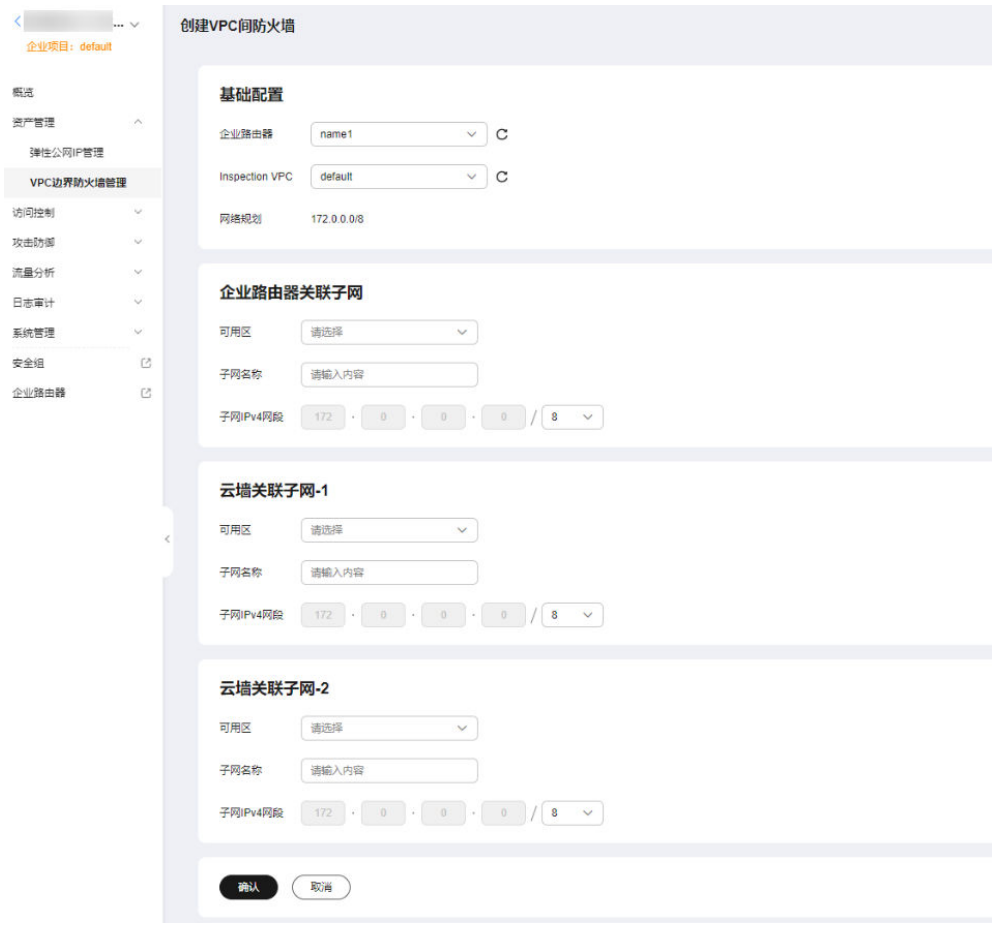
步骤5 在左侧导航栏中，选择“资产管理 > VPC边界防火墙管理”，进入“VPC边界防火墙管理”页面。

步骤6 单击“创建防火墙”，选择企业路由器并配置合适的网段。

图 5-4 创建 VPC 边界防火墙

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

图 5-5 创建 VPC 边界防火墙（旧版）



步骤7 单击“确认”，需等待3-5分钟，完成防火墙创建。

创建过程中您只能浏览“概览”页，防火墙的“状态”会变为“升级中”。

----结束

相关操作

关闭防火墙：防火墙创建后不支持删除和退订，您可以关闭防火墙的防护请参见**关闭VPC边界防护**，如果业务后续不再需要VPC边界流量防护，在关闭后，需要**手动恢复企业路由器（ER）的配置**。

5.2.2 配置企业路由器并将流量引至云防火墙

本文指导您通过企业路由器将流量引至云防火墙，并验证网络的连通性。

前提条件

流量互通，确定流量未经过防火墙时正常通信。流量验证请参见**验证网络互通情况**。

配置原理和流程

配置企业路由器时的流量走势如**图 流量走势图**所示，操作流程如**图 配置企业路由器操作步骤**所示。

图 5-6 流量走势图

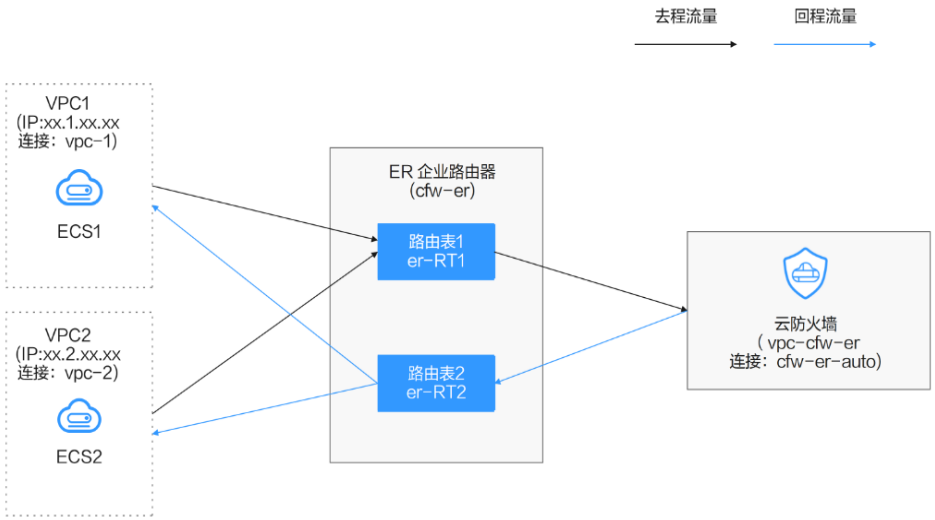
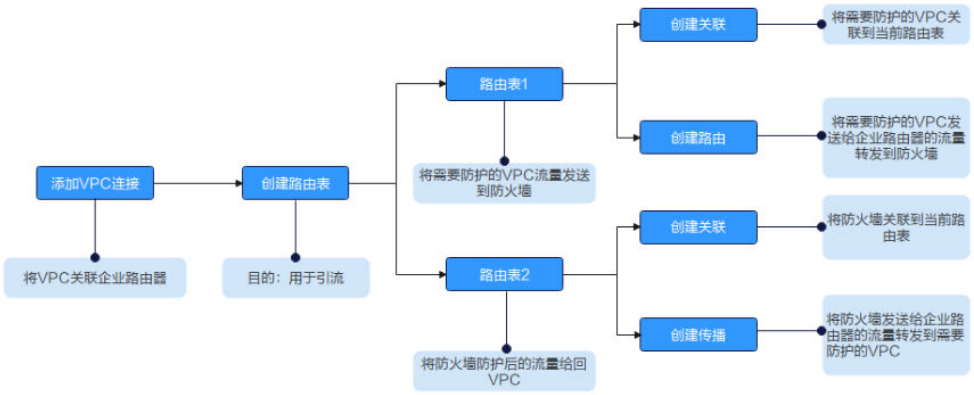


图 5-7 操作流程



将流量引至云防火墙

根据当前业务是否已配置企业路由器，选择配置方式。

通过配置企业路由器将流量引至云防火墙

步骤1 创建VPC边界防火墙，具体操作请参见**创建VPC边界防火墙**。

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

步骤3 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

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

步骤5 添加VPC连接。

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

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

图 5-8 添加 VPC 连接

说明

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

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

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

单击“路由表”页签，进入路由表设置页面，单击“创建路由表”，参数详情见**表 创建路由表参数说明**。

表 5-2 创建路由表参数说明

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

步骤7 配置关联路由表。

1. 设置关联功能：在路由表设置页面，选择关联路由表，单击“关联”页签，单击“创建关联”，参数详情见**表 创建关联参数说明**。

图 5-9 创建关联

表 5-3 创建关联参数说明

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

说明

关联至少需要添加两条，每增加一个防护的VPC，都需增加一条关联。

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

2. 设置路由功能：单击“路由”页签，单击“创建路由”，根据实际数量创建路由功能，参数详情见**表 创建路由参数说明**。

图 5-10 创建路由

表 5-4 创建路由参数说明

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

步骤8 配置传播路由表。

1. 设置关联功能：在路由表设置页面，选择传播路由表，单击“关联”页签，单击“创建关联”，参数详情见**表 创建关联参数说明** 。

图 5-11 创建关联

表 5-5 创建关联参数说明

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

2. 设置传播功能：单击“传播”页签，单击“创建传播”，参数详情见**表 创建传播参数说明**。

图 5-12 创建传播

表 5-6 创建传播参数说明

参数名称	参数说明
连接类型	选择连接类型“虚拟私有云（VPC）”。

参数名称	参数说明
连接	在传播下拉列表中，选择需防护的VPC连接。

说明

- 传播至少需要添加两条，每增加一个防护的VPC，都需增加一条传播。

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

步骤9 修改VPC的路由表。

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

表 5-7 添加路由参数说明

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

说明

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

----结束

修改已有企业路由器将流量引至云防火墙

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

步骤2 **登录管理控制台**。

步骤3 单击管理控制台左上角的，选择区域。

步骤4 在左侧导航栏中，单击左上方的 ，选择“网络 > 企业路由器”，进入“企业路由器”页面。

步骤5 从默认路由表er-RT1中删除防火墙VPC(vpc-cfw-er)的关联和传播。

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

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

步骤6 创建路由表er-RT2。

单击页面左上角“创建路由表”。参数详情见**表 创建路由表参数说明**。

表 5-8 创建路由表参数说明

参数名称	参数说明	取值样例
名称	输入路由表的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	er-RT2
标签	您可以在创建路由表的时候为路由表绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。 关于标签更详细的说明，请参见**标签概述**。	“标签键”：test “标签值”：01
描述	您可以根据需要在文本框中输入对该路由表的描述信息。	-

步骤7 配置路由表er-RT2：设置关联和传播功能。

1. 选择路由表er-RT2，单击“关联”页签，单击“创建关联”。如**图 创建关联**，参数详情见**表 创建关联参数说明** 。

图 5-13 创建关联

表 5-9 创建关联参数说明

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

2. 创建同一路由表(er-RT2)的传播功能。单击“传播”页签，单击“创建传播”。参数详情见**表 创建传播参数说明**。

图 5-14 创建传播

表 5-10 创建传播参数说明

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

表 5-11 创建传播参数说明

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

说明

- 传播至少需要添加两条，每增加一个防护的VPC，都需增加一条传播。

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

步骤8 配置默认路由表er-RT1：

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

图 5-15 添加静态路由

2. 删除路由表er-RT1中的传播。

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

   说明

   需删除路由表er-RT1中所有传播。

步骤9 （可选）建议您将当前企业路由器的传播路由表改为新创建的路由表（er-RT2），后续添加新VPC时，仅需添加连接，无需进行其它操作。

返回或进入“企业路由器”，单击“更多 > 修改配置”，选择传播路由表为er-RT2。如图5-16所示。

图 5-16 修改配置

说明

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

----结束

后续操作

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

5.2.3 开启 VPC 边界防火墙并确认流量经过云防火墙

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

开启 VPC 边界防火墙

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 在“防火墙状态”侧，单击“开启防护”。

步骤7 单击“确认”，完成开启VPC边界防火墙。

----结束

验证流量是否经过云防火墙

步骤1 生成流量，请参见**验证网络互通情况**。

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

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

----结束

后续操作

- 如果您需要添加新的防护VPC，请参见**新增防护VPC**。
- 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**。

5.3 企业路由器模式（旧版）

5.3.1 创建 VPC 边界防火墙

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

前提条件

- 已有企业路由器。

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 配置企业路由器关联子网和云墙关联子网。单击“创建防火墙”，进入“创建VPC间防火墙”页面，配置企业路由器和关联子网信息。

图 5-17 创建 VPC 边界防火墙（旧版）

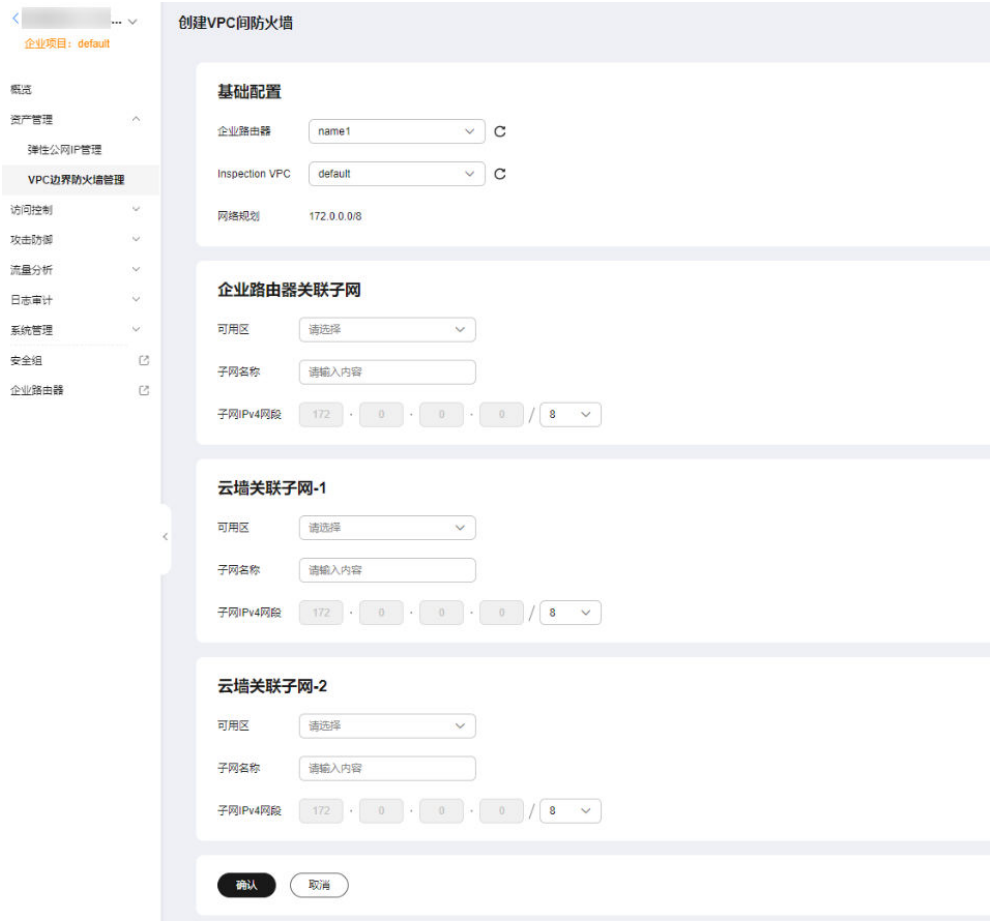


表 5-12 创建 VPC 边界防火墙参数说明

参数名称	参数说明	取值示例
企业路由器	选择您的企业路由器，查看方式请参见**查看企业路由器**。	cfw-er
Inspection VPC	选择VPC。此处的Inspection VPC不能与用于关联企业路由器的其他VPC有重叠网段。	vpc-cfw-er
IPV4网段	选择VPC后自动出现IPV4地址。	xx.xx.0.0/16
可用区	选择可用区。	可用区1
子网名称(企业路由器关联子网）	自定义子网名称。	cfw-er-1
子网名称(云墙关联子网-1）		cfw-er-2
子网名称(云墙关联子网-2）		cfw-er-3
子网IPV4网段(企业路由器关联子网）	分配子网IPV4网段。 **说明** • 需跟现有子网不冲突。 • 三个子网网段之间不冲突。	xx.xx.1.0/24
子网IPV4网段（云墙关联子网-1）		xx.xx.2.0/24
子网IPV4网段(云墙关联子网-2）		xx.xx.3.0/24

步骤7 单击“确认”，需等待3-5分钟，完成防火墙创建。

创建过程中您只能浏览“概览”页，防火墙的“状态”会变为“升级中”。

----结束

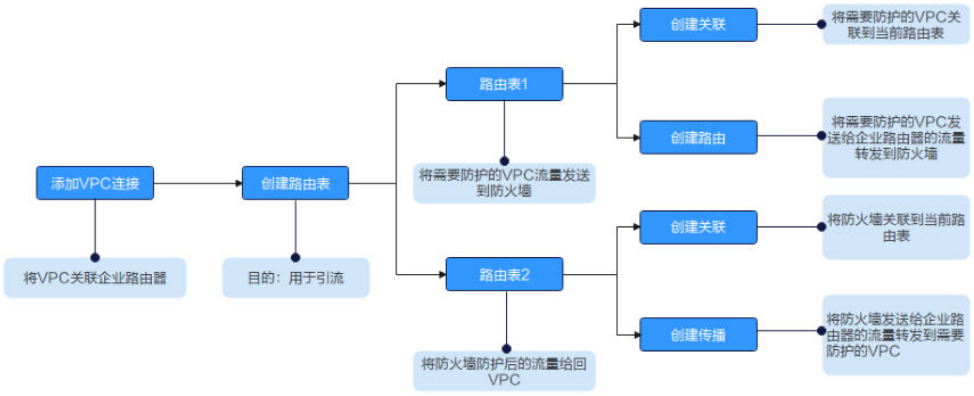
5.3.2 配置企业路由器

防火墙创建完成后，您还需关联企业路由器和设置引流。

配置原理

配置企业路由器时需要执行以下流程。

图 5-18 配置企业路由器操作步骤



前提条件

已完成创建防火墙步骤。

约束条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 单击“配置企业路由器”，进入“企业路由器”页面，在企业路由器中添加连接，支持添加的连接类型请参见**连接概述**。

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

说明

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

步骤7 创建两个路由表分别用于连接需防护的VPC和连接防火墙。

单击“路由表”页签，进入路由表设置页面，单击“创建路由表”。

如图 创建路由表，参数详情见表 创建路由表参数说明。

图 5-19 创建路由表

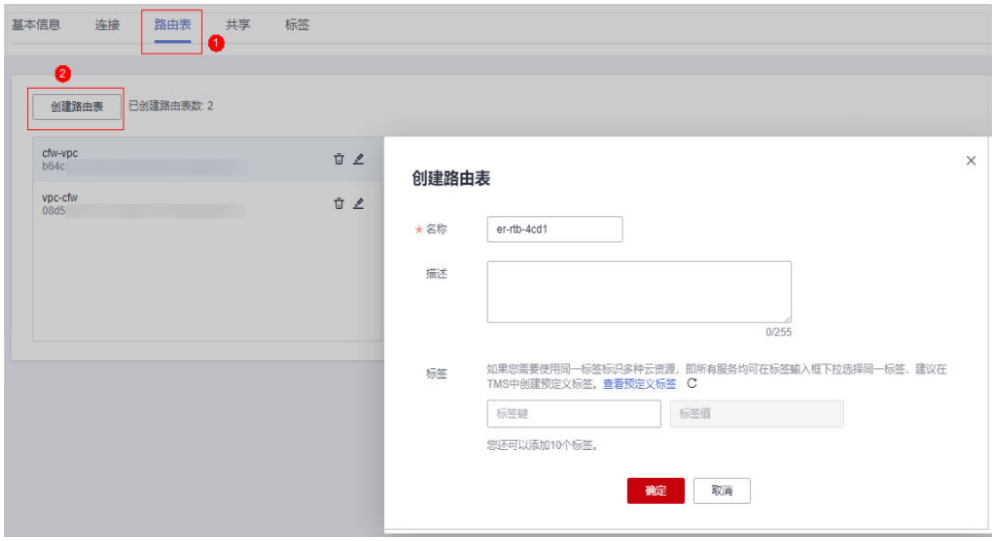


表 5-13 创建路由表参数说明

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

步骤8 设置关联和路由功能。

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

   如图 创建关联，参数详情见表 创建关联参数说明。

图 5-20 创建关联

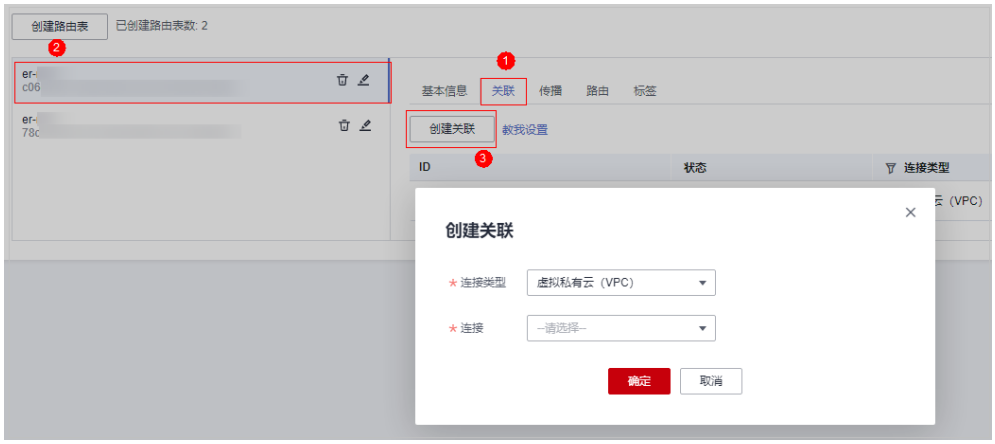


表 5-14 创建关联参数说明

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

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

   如图 创建路由，参数详情见表 创建路由参数说明。

图 5-21 创建路由

表 5-15 创建路由参数说明

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

步骤9 设置关联和传播功能。

1. 在路由表设置页面，单击“关联”页签，选择用于连接防火墙的路由表，单击“创建关联”。
   如**图 创建关联**，参数详情见**表 创建关联参数说明** 。

图 5-22 创建关联

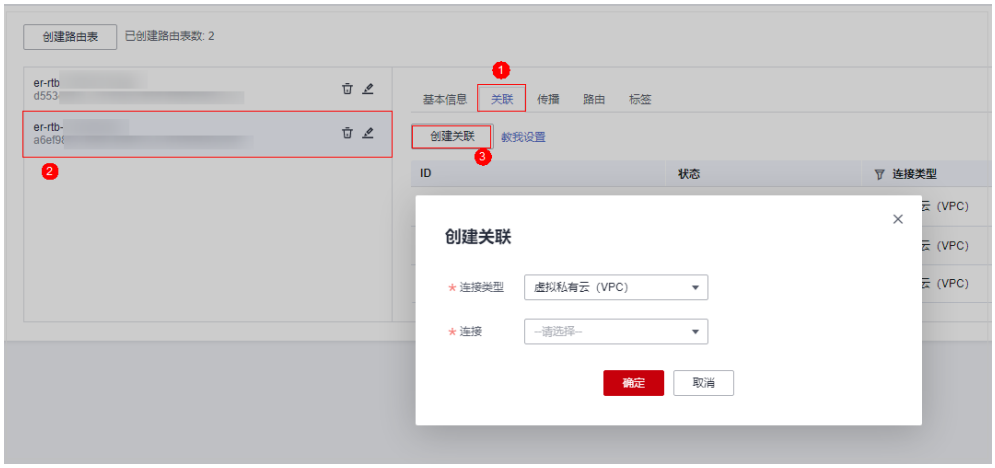


表 5-16 创建关联参数说明

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

2. 创建同一路由表的传播功能。单击“传播”页签，单击“创建传播”。
   如**图 创建传播**，参数详情见**表 创建传播参数说明**。

图 5-23 创建传播

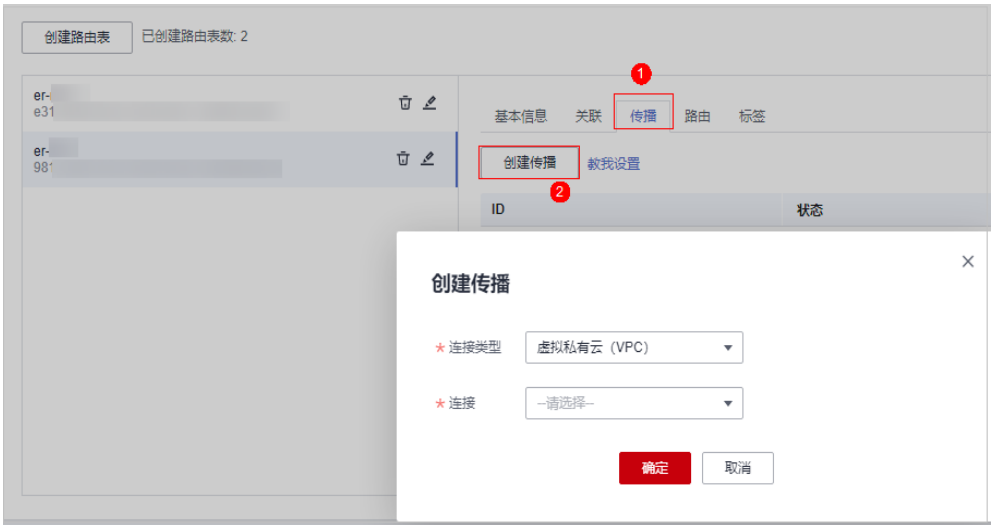


表 5-17 创建传播参数说明

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

说明

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

----结束

配置验证方法

前提条件

- 已完成全部配置步骤。
- 两个VPC中各有一台ECS。

验证方式

VPC中的ECS互相*ping*，确定流量未经过防火墙时是否正常通信。

故障定位

步骤1 企业路由器的两个路由表配置是否正确。正确配置方式请参见**步骤8**和**步骤9**。

步骤2 检查待防护VPC的默认路由表是否将路由转向企业路由器。

查看方式：

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

2、查看是否存在“下一跳类型”为“企业路由器”的路由。若不存在，单击“添加路由”，参数详情见**表 添加路由参数说明**。

表 5-18 添加路由参数说明

参数	说明	取值样例
目的地址	目的地址网段。 目的地址不能与已有路由冲突，目的地址也不能与VPC下子网网段冲突。 **说明** 不能与已有路由和VPC下子网网段冲突。	192.168.0.0/16
下一跳类型	在下拉列表中，选择类型“企业路由器”。	企业路由器
下一跳	选择下一跳资源。 下拉列表中包含资源将基于您所选的资源类型进行展示。	er-01
描述	路由的描述信息，非必填项。 **说明** 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

----结束

5.3.3 开启/关闭 VPC 间边界防火墙

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

前提条件

- 已购买CFW专业版。
- 已配置企业路由器。

约束条件

- 仅专业版支持VPC间防火墙防护功能。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 在“操作”列，单击“开启防护”或“关闭防护”。

----结束

5.4 管理 VPC 边界防火墙

5.4.1 新增防护 VPC

当您配置完成VPC边界防火墙，需要添加防护VPC时，可执行本节操作。

步骤一：添加 VPC 连接

操作步骤请参见企业路由器中添加VPC连接。

说明

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

步骤二：配置关联路由表的关联和传播路由表的传播

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

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

图 5-24 创建关联

表 5-19 创建关联参数说明

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

说明

关联至少需要添加两条，每增加一个防护的VPC，都需增加一条关联。

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

步骤3 设置传播功能：选择传播路由表，单击“传播”页签，单击“创建传播”，参数详情见**表 创建传播参数说明**。

图 5-25 创建传播

表 5-20 创建传播参数说明

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

说明

- 传播至少需要添加两条，每增加一个防护的VPC，都需增加一条传播。

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

----结束

步骤三：修改 VPC 的路由表

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

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

步骤3 单击“添加路由”，参数详情见**表 添加路由参数说明**。

表 5-21 添加路由参数说明

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

说明

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

----结束

5.4.2 关闭 VPC 边界防护

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

如果您的业务后续不再需要VPC边界流量防护，关闭防护后，还需手动恢复企业路由器（ER）的配置，请参见**永久关闭VPC边界防护后恢复企业路由器配置**。

关闭 VPC 边界防火墙（新版）

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 在“防火墙状态”侧，单击“关闭防护”。

步骤7 单击“确认”，完成关闭VPC边界防火墙。关闭后，您VPC边界的流量将不会被防火墙防护。

----结束

关闭 VPC 边界防火墙（旧版）

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 在“操作”列，单击“关闭防护”。

----结束

5.4.3 永久关闭 VPC 边界防护后恢复企业路由器配置

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

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

应用场景

当前业务不再需要VPC边界防火墙防护。

恢复企业路由器配置

步骤1 关闭VPC边界防火墙防护，请参见**关闭VPC边界防护**。

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

步骤3 将传播路由表中的路由（配置传播后自动生成）配置到关联路由表中。

1. 在“关联路由表”的“路由”页签中，单击“创建路由”。参数信息填写“传播路由表”的“路由”配置中防护VPC的“目的地址”和“下一跳”。

   说明

   - 关联路由表：将流量从VPC传输到云防火墙的路由表，配置时的操作请参见**配置关联路由表**。

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

2. （可选）删除“传播路由表”。

   说明

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

3. 删除云防火墙连接，请**提交工单**。

----结束

6 开启 NAT 网关流量防护

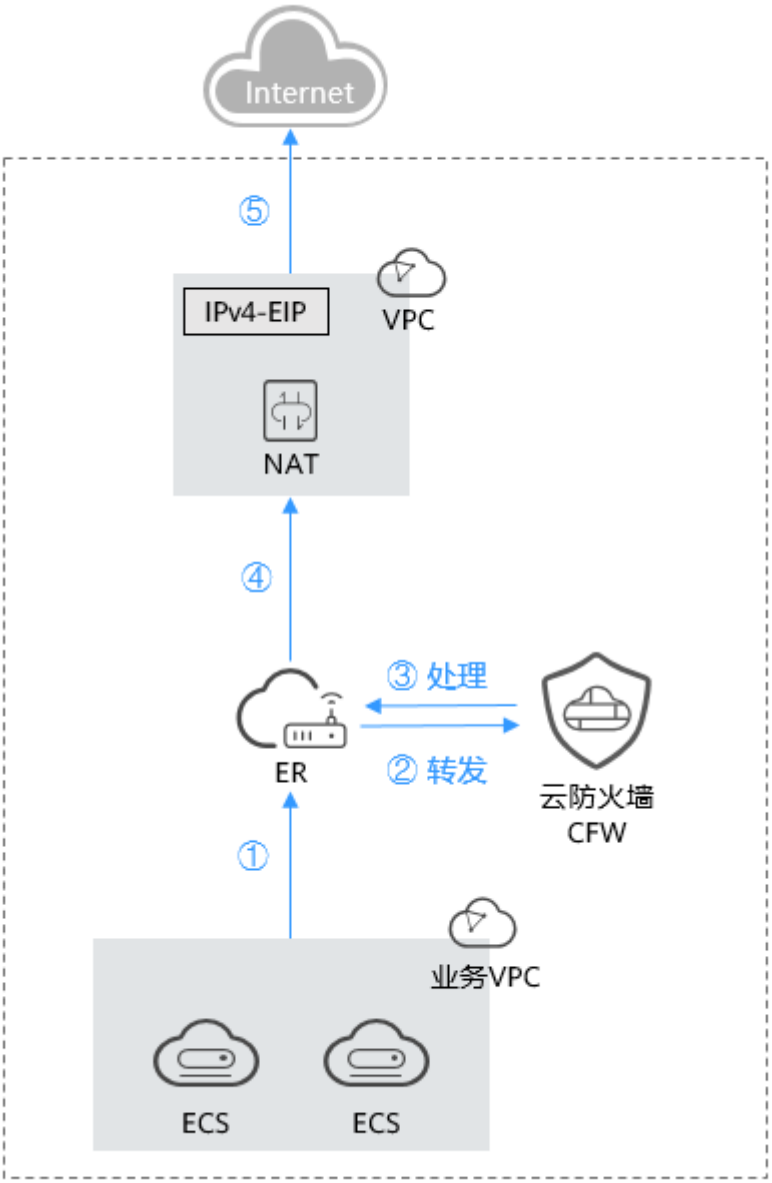
云防火墙通过防护NAT网关所在的VPC，实现对NAT网关流量的防护，并支持对私网IP进行细粒度访问控制，防止内网主机非法外联。

支持防护SNAT和DNAT两种场景。

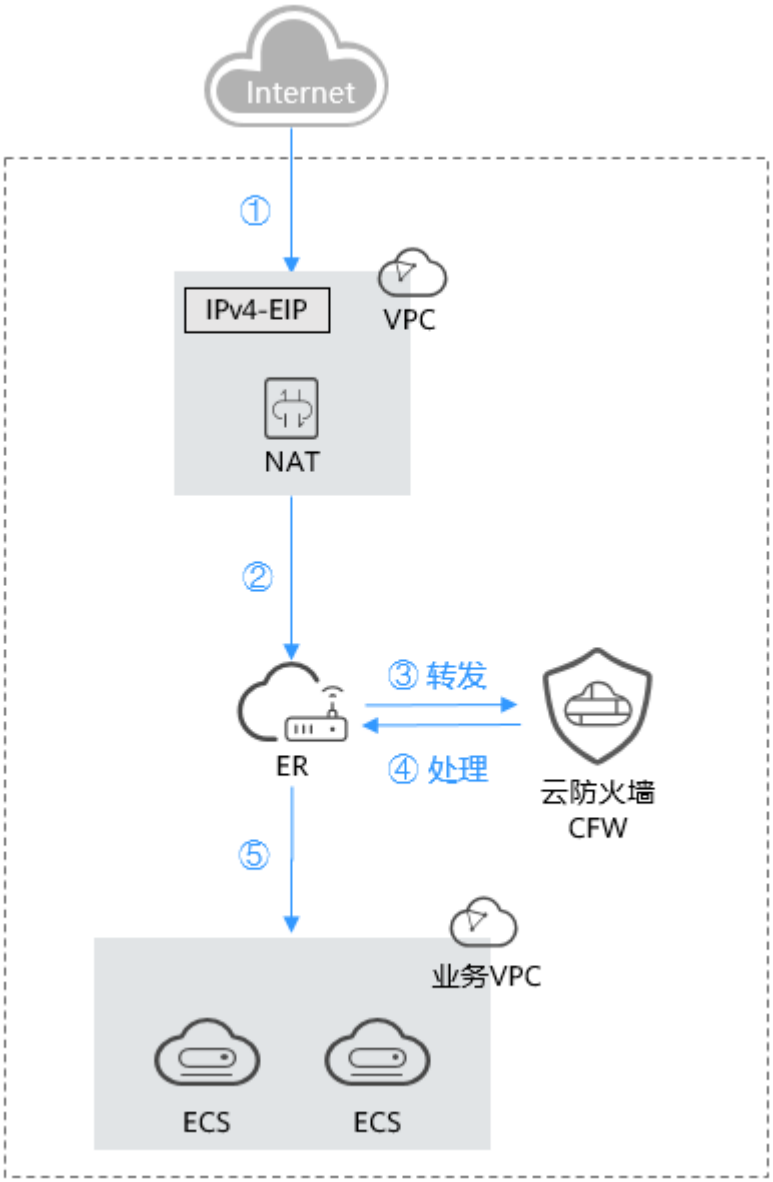
组网图

SNAT和DNAT的组网图如下：

SNAT 组网图



DNAT 组网图



约束条件

- 仅“专业版”支持NAT网关流量防护。
- 依赖企业路由器（Enterprise Router, ER）服务引流。
- 云防火墙当前默认支持标准私网网段，如需开通非标网段通信，请提交工单申请。
- 如要实现DNAT网关向CFW集群东西向引流并配置DNAT规则，需提工单联系服务运维人员支撑防火墙升级，避免因旧版本不支持DNAT可能引起的流量受损风险。

开启 NAT 网关流量防护

需完成创建防火墙，具体配置请参见**创建VPC边界防火墙**。

步骤一：将VPC1和VPC-NAT接入企业路由器中

1. 添加VPC连接。

   操作步骤请参见**企业路由器中添加VPC连接**。

   说明

   连接需要添加两条，“连接资源”分别选择VPC1和VPC-NAT。

2. 创建两个路由表。

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

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

   单击“路由表”页签，进入路由表设置页面，单击“创建路由表”，参数详情见**表 创建路由表参数说明**。

   表 6-1 创建路由表参数说明

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

3. 设置关联路由表。

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

   表 6-2 创建关联参数说明

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

说明

关联需要增加两条，“连接”分别选择VPC1和VPC-NAT的连接。

b. 添加静态路由，指向防火墙：单击“路由”页签，单击“创建路由”，参数详情见**表 创建路由参数说明**。

图 6-1 创建路由

表 6-3 创建路由参数说明

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

4. 设置传播路由表。

a. 设置传播功能，添加VPC1的传播：在路由表设置页面，选择传播路由表，单击“传播”页签，单击“创建传播”，参数详情见**表 创建传播参数说明**。

图 6-2 创建传播

表 6-4 创建传播参数说明

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

b. 添加静态路由，指向VPC-NAT：单击“路由”页签，单击“创建路由”，参数详情见**表 创建路由参数说明**。

表 6-5 创建路由参数说明

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

步骤二：配置NAT网关

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

表 6-6 添加 SNAT 规则

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

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

表 6-7 添加路由参数说明

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

步骤三：配置VPC1路由表

1. 在“路由表”页面的“名称”列，单击VPC1的路由表名称，进入路由表“基本信息”页面。
2. 单击“添加路由”，参数详情见**表 添加路由参数说明**。

表 6-8 添加路由参数说明

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

步骤四：开启VPC边界防火墙

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

后续操作

- 实现私网IP的细粒度防护：配置NAT防护规则，配置方式请参见**NAT流量防护规则**。
- 实现网络攻击拦截：配置入侵防御功能，请参见**拦截网络攻击**。

7 配置访问控制策略管控流量

7.1 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，各功能的防护顺序请参见**云防火墙的防护顺序是什么？**。

表 7-1 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	• 五元组 • IP地址组 • 地理位置（地域） • 域名和域名组	• 公网IP • 私网IP	• 设置为“阻断”：流量直接拦截。 • 设置为“放行”：流量被“防护规则”功能放行后，再经过入侵防御（IPS）功能检测。	**通过添加防护规则拦截/放行流量**
黑名单	• 五元组 • IP地址组		直接拦截流量。	**通过添加黑白名单拦截/放行流量**
白名单			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（如内容分发网络（CDN）、DDoS高防、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	• 80 • 443	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**。

7.2 通过配置防护规则拦截/放行流量

7.2.1 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**什么是回源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、扩容引擎）需要客户端重新发起连接。相关问题建议**提交工单**评估风险。
- 配额限制：
  - 最多添加20,000条防护规则。
  - 单条防护规则最大限制如下：
    - 最多添加20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。
  - 网络型域名组最多只能保存1000个地址解析结果，超出时，可能导致无法正常访问对应的域名；对于解析结果较多或变化频繁的域名，如果防护流量是HTTP、HTTPS协议，建议优先使用应用型域名组添加策略。
  - 域名防护依赖于用户配置的域名服务器。默认域名服务器可能存在域名解析对应的IP地址不全，建议有访问自身业务相关域名场景时配置**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”。
- 开启NAT64防护后，使用IPv6访问时，请注意将198.19.0.0/16的网段放通。因为NAT64会将源IP转换成198.19.0.0/16的网段进行ACL访问控制。

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。

添加防护规则

参考以下操作添加对应场景的防护规则。

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 7-2 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“EIP规则”：防护EIP的流量，仅支持配置公网IP；配置私网IP请参见**NAT流量防护规则**。 **说明** 标准版防火墙默认配置EIP规则，不支持选择“规则类型”参数。
名称	自定义安全策略规则的名称。
方向	“防护规则”选择EIP规则时，需要选择流量的方向： ● 外-内：互联网访问云上资产（EIP）。 ● 内-外：云上资产（EIP）访问互联网。
源	设置会话发起方。 ● IP地址：填写公网IP地址，支持设置单个IP地址、多个连续IP地址、地址段。 – 单个公网IP地址，如：xx.xx.10.5 – 多个连续的公网IP地址，中间使用“-”隔开，如：xx.xx.0.2-xx.xx.0.10 – 公网IP地址段，使用"/"隔开掩码，如：xx.xx.2.0/24 ● IP地址组：支持多个公网IP地址的集合，添加自定义IP地址组请参见**添加IP地址组**，预定义地址组请参见**查看预定义地址组**。 **说明** “方向”配置为“外-内”时，“源”地址支持配置“预定义地址组”。 ● 地域：“方向”选择“外-内”时，支持地理位置防护，通过指定大洲、国家、地区配置防护规则。 ● Any：任意源地址。

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

参数名称	参数说明
服务	• 服务：设置协议类型、源端口和目的端口。 – 协议类型：支持选择TCP、UDP、ICMP。 – 源/目的端口：“协议类型”选择“TCP”或“UDP”时，需要设置端口号。 **说明** – 如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。 – 如您需设置某个端口，可填写为单个端口。例如设置22端口的访问，则配置“端口”为“22”。 – 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如设置80-443端口的访问，则配置“端口”为“80-443”。 • 服务组：支持多个服务（协议、源端口、目的端口）的集合，添加自定义服务组请参见**添加服务组**，预定义服务组请参见**查看预定义服务组**。 • Any：任意协议类型和端口号。
应用	（可选，“目的”选择“域名/域名组”时，参数为必选）设置针对应用层协议的防护策略。 • “服务”选择“Any”时，支持所有应用类型。 • “服务”选择“服务”，“协议类型”选择“TCP”时，支持TCP的应用类型，如HTTP、HTTPS等。 • “服务”选择“服务”，“协议类型”选择“UDP”时，支持UDP的应用类型，如DNS、RDP等。
防护动作	设置流量经过防火墙时的处理动作。 • 放行：防火墙允许此流量转发。 • 阻断：防火墙禁止此流量转发。
启用状态	设置该策略是否立即启用。  ：表示立即启用，规则生效。  ：表示立即关闭，规则不生效。
策略优先级	设置该策略的优先级： • 置顶：表示将该策略的优先级设置为最高。 • 移动至选中规则后：表示将该策略优先级设置到某一规则后。 **说明** • 设置后，优先级数字越小，策略的优先级越高。 • 添加的第一条防护规则默认优先级是1，无需选择“策略优先级”。
时间计划管理	（可选）单击“时间计划管理”设置规则的生效时间段，选择已设置的时间计划或**新增时间计划**。

参数名称	参数说明
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。 ● 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50条规则设置长连接。
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”。 **说明** 支持时长设置为1秒~1000天。
标签	（可选）用于标识规则，可通过标签实现对安全策略的分类和搜索。
描述	（可选）标识该规则的使用场景和用途，以便后续运维时快速区分不同规则的作用。

步骤4 单击“确认”，完成配置防护规则。

----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 7-3 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。

参数名称	参数说明
源	设置会话发起方。 ● IP地址：支持设置单个IP地址、多个连续IP地址、地址段。 – 单个IP地址，如：192.168.10.5 – 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 ● IP地址组：支持多个IP地址的集合，添加IP地址组请参见**添加IP地址组**。 ● Any：任意源地址。
目的	设置会话接收方。 ● IP地址：支持设置单个IP地址、多个连续IP地址、地址段。 – 单个IP地址，如：192.168.10.5 – 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 ● IP地址组：支持多个IP地址的集合，添加IP地址组请参见**添加IP地址组**。 ● 域名/域名组：支持域名或域名组的防护。 应用型：支持**域名**或**泛域名**的防护；适用应用层协议，支持HTTP、HTTPS的应用协议类型；通过域名匹配。 ● Any：任意目的地址。
服务	设置访问流量的“协议类型”和“端口号”。 ● 服务：设置协议类型、源端口和目的端口。 – 协议类型：支持选择TCP、UDP、ICMP。 – 源/目的端口：“协议类型”选择“TCP”或“UDP”时，需要设置端口号。 **说明** – 如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。 – 如您需设置某个端口，可填写为单个端口。例如设置22端口的访问，则配置“端口”为“22”。 – 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如设置80-443端口的访问，则配置“端口”为“80-443”。 ● 服务组：支持多个服务（协议、源端口、目的端口）的集合，添加自定义服务组请参见**添加服务组**，预定义服务组请参见**查看预定义服务组**。 ● Any：任意协议类型和端口号。

参数名称	参数说明
应用	（可选）设置针对应用层协议的防护策略。 ● “服务”选择“Any”时，支持所有应用类型。 ● “服务”选择“服务”，“协议类型”选择“TCP”时，支持TCP的应用类型，如HTTP、HTTPS等。 ● “服务”选择“服务”，“协议类型”选择“UDP”时，支持UDP的应用类型，如DNS、RDP等。
防护动作	设置流量经过防火墙时的处理动作。 ● 放行：防火墙允许此流量转发。 ● 阻断：防火墙禁止此流量转发。
启用状态	设置该策略是否立即启用。  ：表示立即启用，规则生效。  ：表示立即关闭，规则不生效。
策略优先级	设置该策略的优先级： ● 置顶：表示将该策略的优先级设置为最高。 ● 移动至选中规则后：表示将该策略优先级设置到某一规则后。 **说明** ● 设置后，优先级数字越小，策略的优先级越高。 ● 添加的第一条防护规则默认优先级是1，无需选择“策略优先级”。
时间计划管理	（可选）单击“时间计划管理”设置规则的生效时间段，选择已设置的时间计划或**新增时间计划**。
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。 ● 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50条规则设置长连接。
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”。 **说明** 支持时长设置为1秒~1000天。
标签	（可选）用于标识规则，可通过标签实现对安全策略的分类和搜索。
描述	（可选）标识该规则的使用场景和用途，以便后续运维时快速区分不同规则的作用。

步骤4 单击“确认”，完成配置防护规则。

----结束

NAT 流量防护规则

步骤1 开启NAT流量防护，请参见**开启NAT网关流量防护**。

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

步骤3 添加新的防护规则。

单击“添加”，在弹出的“添加防护规则”中，填写新的防护信息。

- DNAT场景填写规则请参见**表 添加防护规则-DNAT场景**
- SNAT场景填写规则请参见**表 添加防护规则-SNAT场景**。

表 7-4 添加防护规则-DNAT 场景

参数名称	参数说明
规则类型	选择NAT规则： 防护NAT网关的流量，支持配置私网IP。 **说明** NAT规则需满足： • “专业版”防火墙，升级版本请参见**升级云防火墙版本**。 • 已配置VPC边界防火墙，请参见**管理VPC边界防火墙**。
名称	自定义安全策略规则的名称。
方向	选择“DNAT”。
源	设置会话发起方。 • IP地址：填写私网IP地址，支持设置单个IP地址、多个连续IP地址、地址段。 – 单个IP地址，如：192.168.10.5 – 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 • IP地址组：支持多个私网IP地址的集合，添加IP地址组请参见**添加IP地址组**。 • 地域：支持地理位置防护，通过指定大洲、国家、地区配置防护规则。 • Any：任意源地址。

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

参数名称	参数说明
策略优先级	设置该策略的优先级： ● 置顶：表示将该策略的优先级设置为最高。 ● 移动至选中规则后：表示将该策略优先级设置到某一规则后。 **说明** ● 设置后，优先级数字越小，策略的优先级越高。 ● 添加的第一条防护规则默认优先级是1，无需选择“策略优先级”。
时间计划管理	（可选）单击“时间计划管理”设置规则的生效时间段，选择已设置的时间计划或**新增时间计划**。
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。 ● 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50条规则设置长连接。
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”。 **说明** 支持时长设置为1秒~1000天。
标签	（可选）用于标识规则，可通过标签实现对安全策略的分类和搜索。
描述	（可选）标识该规则的使用场景和用途，以便后续运维时快速区分不同规则的作用。

表 7-5 添加防护规则-SNAT 场景

参数名称	参数说明
规则类型	选择NAT规则： 防护NAT网关的流量，支持配置私网IP。 **说明** NAT规则需满足： ● “专业版”防火墙，升级版本请参见**升级云防火墙版本**。 ● 已配置VPC边界防火墙，请参见**管理VPC边界防火墙**。
名称	自定义安全策略规则的名称。
方向	选择“SNAT”。

参数名称	参数说明
源	设置会话发起方。 ● IP地址：填写私网IP地址，支持设置单个IP地址、多个连续IP地址、地址段。 – 单个IP地址，如：192.168.10.5 – 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 ● IP地址组：支持多个私网IP地址的集合，添加IP地址组请参见**添加IP地址组**。 ● 地域：支持地理位置防护，通过指定大洲、国家、地区配置防护规则。 ● Any：任意源地址。
目的	设置会话接收方。 ● IP地址：填写私网IP地址，支持设置单个IP地址、多个连续IP地址、地址段。 – 单个IP地址，如：192.168.10.5 – 多个连续IP地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 – 地址段，使用"/"隔开掩码，如：192.168.2.0/24 ● IP地址组：支持多个私网IP地址的集合，添加IP地址组请参见**添加自定义IP地址组**。 ● 地域：支持地理位置防护，通过指定大洲、国家、地区配置防护规则。 ● 域名/域名组：“方向”选择“内-外”时，支持域名或域名组的防护。 – 应用型：支持**域名**或**泛域名**的防护；适用应用层协议，支持HTTP、HTTPS的应用协议类型；通过域名匹配。 – 网络型：支持**单个域名**或**多个域名**的防护；适用网络层协议，支持所有协议类型；通过解析到的IP过滤。 **说明** – 防护HTTP、HTTPS应用类型的**域名**时可选择任意类型。 – 防护HTTP、HTTPS应用类型的**泛域名**时仅支持选择“应用型”的任意选项。 – 防护其它应用类型（如FTP、MySQL、SMTP）的**单个域名**：选择“网络型”的任意选项（选择“域名”时，解析出的ip地址上限个数为600个）。 – 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”。 – 应用型与网络型详细介绍请参见**添加域名组**。 ● Any：任意目的地址。

参数名称	参数说明
服务	• 服务：设置协议类型、源端口和目的端口。 – 协议类型：支持选择TCP、UDP、ICMP。 – 源/目的端口：“协议类型”选择“TCP”或“UDP”时，需要设置端口号。 **说明** – 如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。 – 如您需设置某个端口，可填写为单个端口。例如设置22端口的访问，则配置“端口”为“22”。 – 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如设置80-443端口的访问，则配置“端口”为“80-443”。 • 服务组：支持多个服务（协议、源端口、目的端口）的集合，添加自定义服务组请参见**添加服务组**，预定义服务组请参见**查看预定义服务组**。 • Any：任意协议类型和端口号。
应用	（可选，“目的”选择“域名/域名组”时，参数为必选）设置针对应用层协议的防护策略。 • “服务”选择“Any”时，支持所有应用类型。 • “服务”选择“服务”，“协议类型”选择“TCP”时，支持TCP的应用类型，如HTTP、HTTPS等。 • “服务”选择“服务”，“协议类型”选择“UDP”时，支持UDP的应用类型，如DNS、RDP等。
防护动作	设置流量经过防火墙时的处理动作。 • 放行：防火墙允许此流量转发。 • 阻断：防火墙禁止此流量转发。
启用状态	设置该策略是否立即启用。  ：表示立即启用，规则生效。  ：表示立即关闭，规则不生效。
策略优先级	设置该策略的优先级： • 置顶：表示将该策略的优先级设置为最高。 • 移动至选中规则后：表示将该策略优先级设置到某一规则后。 **说明** • 设置后，优先级数字越小，策略的优先级越高。 • 添加的第一条防护规则默认优先级是1，无需选择“策略优先级”。
时间计划管理	（可选）单击“时间计划管理”设置规则的生效时间段，选择已设置的时间计划或**新增时间计划**。

参数名称	参数说明
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。 • 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50条规则设置长连接。
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”。 **说明** 支持时长设置为1秒~1000天。
标签	（可选）用于标识规则，可通过标签实现对安全策略的分类和搜索。
描述	（可选）标识该规则的使用场景和用途，以便后续运维时快速区分不同规则的作用。

步骤4 单击“确认”，完成配置防护规则。

说明

访问控制策略默认状态为放行。

----结束

后续操作

查看防护效果：

- 策略的命中情况，整体防护概况请参见**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**。

相关操作

批量添加防护规则请参见**导入/导出防护策略**。

7.2.2 示例一：放行入方向中指定 IP 的访问流量

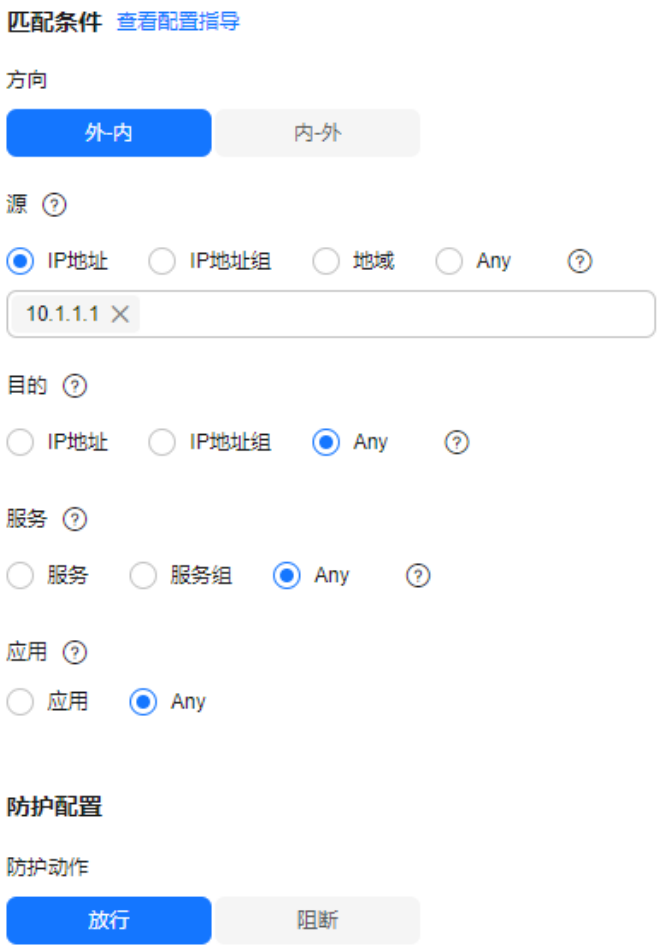
本文提供放行入方向中指定IP访问流量的配置示例，更多参数配置请参见**通过添加防护规则拦截/放行流量**。

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，如**图 拦截所有流量**所示，优先级置于最低，一条单独放行指定IP的流量访问，如**图 放行指定IP**所示，优先级设置最高，其余参数可根据您的部署进行填写。

图 7-1 拦截所有流量

图 7-2 放行指定 IP



7.2.3 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“新加坡”地区的访问流量，可以参照以下参数设置防护规则。

图 7-3 拦截新加坡地区的访问流量

7.2.4 示例三：放行业务访问某平台的流量

本文提供放行业务访问某平台的流量的配置示例，更多参数配置请参见**通过添加防护规则拦截/放行流量**。

放行业务访问某平台的流量

假如您需要放行EIP（xx.xx.xx.48）对“cfw-test.com”和“*.example.com”的访问流量，设置参数如下，其余参数可根据您的部署进行填写。

- 将平台域名添加至应用型域名组，如**图 添加某平台域名组**所示。
- 配置两条防护规则：
  - 一条拦截所有流量，如**图 拦截所有流量**所示，优先级置于最低。
  - 一条放行EIP对某平台的流量访问，如**图 放行IP对某平台的访问流量**所示，优先级设置最高。

图 7-4 添加某平台域名组

图 7-5 拦截所有流量

图 7-6 放行 EIP 对某平台的访问流量

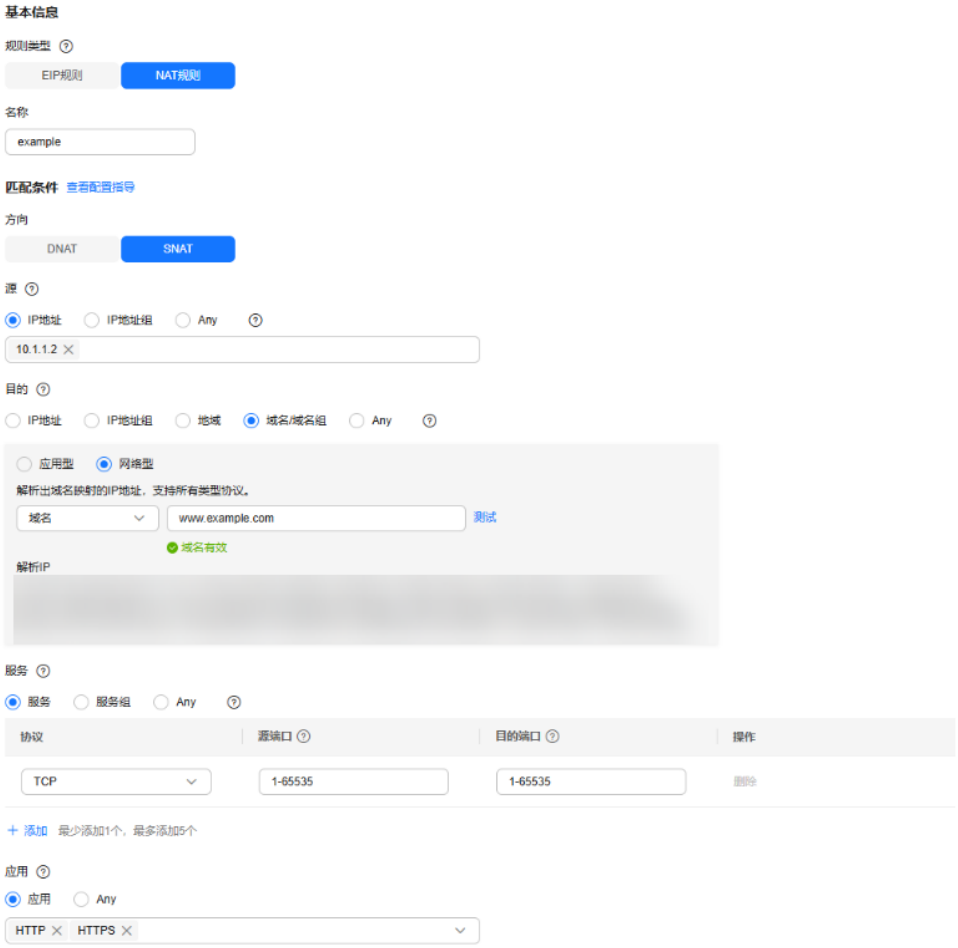
7.2.5 示例四：配置 SNAT 的防护规则

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

SNAT 防护配置

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

图 7-7 添加 NAT 防护规则



7.3 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**什么是回源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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 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7-6**。

表 7-6 黑/白名单

参数名称	参数说明
地址方向	选择“源地址”或“目的地址”。 ● 源地址：设置会话发起方。 ● 目的地址：设置会话接收方。
协议类型	协议类型当前支持：TCP、UDP、ICMP、Any。
端口	“协议类型”选择“TCP”或“UDP”时，设置需要放行或拦截的端口。 **说明** ● 如您需设置该IP地址的全部端口，可配置“端口”为“1-65535”。 ● 如您需设置某个端口，可填写为单个端口。例如放行/拦截该IP地址22端口的访问，则配置“端口”为“22”。 ● 如您需设置某个范围的端口，可填写为连续端口组，中间使用“-”隔开。例如放行/拦截该IP地址80-443端口的访问，则配置“端口”为“80-443”。
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	• 自定义IP地址：在输入框中输入单个或多个IP地址，单击“解析”，将IP地址加入列表中。 • 预定义地址组：单击“添加预定义地址组”，在弹出的对话框中选择地址组，预定义地址组介绍请参见**预定义地址组**。 **注意** “WAF回源IP地址组”添加至黑/白名单后，如果回源IP改变，您需手动修改对应黑/白名单中的IP地址。

步骤7 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**。

7.4 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 策略助手”，进入“策略助手”页面。

步骤6 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 7-7 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

7.5 访问控制策略管理

7.5.1 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤6 单击页面右上方“下载中心”，右侧弹出“下载中心”页面。

步骤7 单击“下载模板”，下载导入规则模板到本地。

步骤8 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9 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10 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11 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤6 单击页面右上方“下载中心”，右侧弹出“下载中心”页面。

步骤7 单击“导出规则”，导出规则到本地。

----结束

导入规则模板参数

参考以下参数说明填写模板。

导入规则模板参数-防护规则表（互联网边界防护规则）

表 7-8 互联网边界防护规则表参数说明

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

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

参数名称	参数说明	取值样例
目的IP地址	“目的地址类型”选择“IP地址”时，需填写“目的IP地址”。 目的IP地址支持以下输入格式： ● 单个IP地址，如：192.168.10.5 ● 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10 ● 地址段，使用“/”隔开掩码，如：192.168.2.0/24 **说明** 如果您希望输入多个单IP地址或多个IP地址段，需要配置多条规则。这些规则的IP地址（段）不同，其他参数相同。	192.168.10.6
目的地址组名称	“目的地址类型”选择“IP地址组”时，需填写“目的地址组名称”。 支持以下输入格式； ● 可输入中文、字母、数字、下划线、连接符或空格。 ● 名称长度不能超过255个字符。	d_test
目的大洲地域	“目的地址类型”选择“地域”时，需填写“目的大洲地域”。 您可以切换模板表格至“大洲信息表”页签，查看大洲信息。	AS:亚洲
目的国家地域	“目的地址类型”选择“地域”时，需填写“目的国家地域”。 您可以切换模板表格至“国家信息表”页签，查看国家信息。	CN:中国大陆
域名	“目的地址类型”选择“域名”时，需填写“域名”。 由一串用点分隔的英文字母组成（以字符串的形式来表示服务器IP），用户通过域名来访问网站。	www.example.com
目的域名组名称	“目的地址类型”选择“域名组”时，需填写“目的域名组名称”。 输入域名组名称。	域名组1
服务类型	选择**服务**或**服务组**。 ● **服务**：支持设置单个服务。 ● **服务组**：支持多个服务的集合。	服务

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。 ● 协议类型当前支持：TCP、UDP、ICMP、Any。 ● 设置需要开放或限制的源端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443 ● 设置需要开放或限制的目的端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443	TCP/443/443
服务组名称	自定义服务组名称。 只能由中文、字母、数字、下划线、连接符或空格任意一种或多种字符类型组成，且名称长度不能超过255个字符。	service_test
应用列表	设置应用类型，例如HTTP、HTTPS、DNS、RDP等。	HTTP
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 7-9 VPC 边界防护规则表参数说明

参数名称	参数说明	取值样例
顺序	定义规则序号。	1
规则名称	自定义规则名称。 只能由中文、字母、数字、下划线、连接符或空格任意一种或多种字符类型组成，且名称长度不能超过255个字符。	test
动作	选择“放行”或者“阻断”。设置防火墙对通过流量的处理动作。	放行
启用状态	选择该策略是否立即启用。 ● 启用：表示启用，规则生效； ● 禁用：表示关闭，规则不生效。	启用
描述	自定义规则描述。	test
源地址类型	设置会话发起方的类型。 ● **IP地址**：支持设置单个IP地址、连续多个IP地址、地址段。 ● **IP地址组**：支持多个IP地址的集合。	IP地址

参数名称	参数说明	取值样例
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 **说明** 如果您希望输入多个单IP地址或多个IP地址段，需要配置多条规则。这些规则的IP地址（段）不同，其他参数相同。	192.168.10.5
源地址组名称	“源地址类型”选择“IP地址组”时，需填写“源地址组名称”。 支持以下输入格式； ● 可输入中文、字母、数字、下划线、连接符或空格。 ● 名称长度不能超过255个字符。	s_test
目的地址类型	选择会话接收方的类型。 ● **IP地址**：支持设置单个IP地址、连续多个IP地址、地址段。 ● **IP地址组**：支持多个IP地址的集合。	IP地址组
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 **说明** 如果您希望输入多个单IP地址或多个IP地址段，需要配置多条规则。这些规则的IP地址（段）不同，其他参数相同。	192.168.10.6
目的地址组名称	“目的地址类型”选择“IP地址组”时，需填写“目的地址组名称”。 支持以下输入格式； ● 可输入中文、字母、数字、下划线、连接符或空格。 ● 名称长度不能超过255个字符。	d_test

参数名称	参数说明	取值样例
服务类型	选择**服务**或**服务组**。 • **服务**：支持设置单个服务。 • **服务组**：支持多个服务的集合。	服务
协议/源端口/目的端口	设置需要限制的类型。 • 协议类型当前支持：TCP、UDP、ICMP、Any。 • 设置需要开放或限制的源端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443 • 设置需要开放或限制的目的端口。支持设置单个端口，或者连续端口组，中间使用“-”隔开，如：80-443	TCP/443/443
服务组名称	自定义服务组名称。 只能由中文、字母、数字、下划线、连接符或空格任意一种或多种字符类型组成，且名称长度不能超过255个字符。	service_test
应用列表	设置应用类型，例如HTTP、HTTPS、DNS、RDP等。	HTTP
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

7.5.2 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤6 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7 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8 单击“确认”，完成设置优先级。

----结束

7.5.3 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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 7-10 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/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	访问流量中的会话发起方。
目的	访问流量中的会话接收方。

参数名称	参数说明
服务	• 协议类型当前支持：TCP、UDP、ICMP、Any。 • 源端口：当前开放或限制的源端口号。支持单个端口，或者连续端口组，中间使用“-”隔开，如：80-443。 • 目的端口：当前开放或限制的目的端口号。支持单个端口，或者连续端口组，中间使用“-”隔开，如：80-443。
应用	访问流量中的应用类型。
动作	• “放行”：设置相应流量通过防火墙。 • “阻断”：阻止相应流量通过防火墙。
命中次数	当前规则已放行或阻断的累计命中次数（距上一次清零前），命中详情请参见**访问控制日志**。
时间计划	设置的规则生效时间。
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6 （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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤6 在需要编辑的防护规则所在行的“操作”列，单击“编辑”。

步骤7 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8 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤6 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7 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。

步骤6 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7 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

7.5.4 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 在需要编辑的规则所在行的“操作”列中，单击“编辑”。

对参数进行修改，参数详情请参见**表7-11**。

表 7-11 黑/白名单

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

步骤7 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 在需要删除的规则所在行的“操作”列，单击“删除”。

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

警告

删除名单后无法恢复，请谨慎操作。

----结束

7.5.5 管理时间计划

您可以通过设置防护规则的生效时间段，确保规则仅在指定的时间段内生效。

本节介绍如何添加、复制、删除时间计划。

应用场景

- 配置测试策略：为测试策略设置生效时间段，在测试期间，策略自动生效，确保测试的顺利进行；在测试结束时，策略会自动失效，无需手动操作。
- 控制公网暴露：当业务需要对外部开放端口时（例如仅办公时间开放），设置生效时间段可以有效减少公网暴露，降低潜在的安全风险。
- 特殊时间段的临时需求：临时的公网放行需求，无需担心忘记删除的安全风险。

添加时间计划

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”页面。

步骤6 切换至“时间计划”页签，单击“添加时间计划”，弹出“添加时间计划”界面，填写参数信息。

表 7-12 时间计划参数说明

参数名称	参数说明
时间计划名称	自定义时间计划的名称。
描述	（可选）标识该计划的使用场景和用途，以便后续运维时快速区分不同计划的作用。

参数名称		参数说明
周期计划	添加周期计划	（可选）设置后，规则将在每周的固定时间段生效。 **说明** 当资源所在时区和本地时区不一致时，需要配置“资源所在时区”，即当前region所属地区的时区。
绝对计划	时间设置方式	当资源所在时区和本地时区不一致时，需要选择“时间设置方式”。防火墙引擎执行时按照“资源所在时区”的时间执行。 ● 本地时区：当前客户端浏览器所属时区 。 ● 资源所在时区：云防火墙引擎所在地，即当前region所属地区的时区。
绝对计划	开始时间	设置规则生效的时间。
	结束时间	（可选）设置规则失效的时间。

步骤7 单击“确认”，完成添加。

----结束

后续操作

时间计划添加完成后需在防护规则里设置才会生效，添加防护规则请参见**通过添加防护规则拦截/放行流量**。

相关操作

- 复制时间计划：在目标计划所在行的“操作”列中，单击“复制”，
- 编辑时间计划：单击目标计划的名称，在弹窗中修改参数，单击“确认”。
- 删除时间计划：
  - 删除单个时间计划：在目标计划所在行的“操作”列中，单击“删除”，确认删除的信息无误后，输入“DELETE”，单击“确定”，完成删除。
  - 删除多个时间计划：勾选目标任务，单击列表上方的“删除”，确认删除的信息无误后，输入“DELETE”，单击“确定”，完成删除时间计划。

  说明

  该时间计划被防护规则引用时，不支持删除。

7.6 IP 地址组管理

7.6.1 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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 7-13 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。
IP地址列表	添加需要管理的IP地址，单击“解析”至IP地址列表中。 输入规则如下： • 单个IP地址，如：192.168.10.5。 • 地址段，使用"/"隔开掩码，如：192.168.2.0/24。 • 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10。 • 支持多个IP地址，使用半角逗号（,）、半角分号（;）、换行符、制表符或空格隔开，如192.168.1.0,192.168.1.0/24。

步骤7 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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7 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。

  输入规则如下：

  - 单个IP地址，如：192.168.10.5。
  - 地址段，使用"/"隔开掩码，如：192.168.2.0/24。
  - 多个连续地址，中间使用“-”隔开，如：192.168.0.2-192.168.0.10。
  - 支持多个IP地址，使用半角逗号（,）、半角分号（;）、换行符、制表符或空格隔开，如192.168.1.0,192.168.1.0/24。
- 添加单个IP地址：在列表中单击“添加”，输入“IP地址”和“描述”信息。

步骤8 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**。

7.6.2 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。IPv6转换功能请参见**IPv6转换**。

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，回源IP的相关信息请参见**什么是回源IP?**。

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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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

7.6.3 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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7 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。

警告

删除IP地址组后无法恢复，请谨慎操作。

----结束

7.7 域名组管理

7.7.1 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（如被内容分发网络（CDN）加速的域名）。

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40,000次，泛域名被“防护规则”引用最多200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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 （可选）如果添加网络域名组，则选择“网络域名组”页签。

步骤7 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 7-14 添加域名组参数说明

参数名称	参数说明
域名组类型	应用型/网络型
域名组名称	自定义域名组名称。
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： • 支持多级别单域名（例如，一级域名example.com，二级域名www.example.com等）和泛域名（例如，*.example.com）。 • 多个域名以英文逗号、英文分号、换行符、空格分隔。 **说明** 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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7 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8 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”。

7.7.2 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 （可选）如删除网络域名组，则选择“网络域名组”页签。

步骤7 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

7.8 服务组管理

7.8.1 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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 7-15 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。

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

步骤7 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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7 单击“添加服务”，弹出“添加服务”对话框。

表 7-16 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 **说明** 协议选择ICMP时，无需填写端口号。	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 **说明** 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8 单击添加可添加多个服务。

步骤9 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**。

7.8.2 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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

7.8.3 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“访问控制 > 对象组管理”，进入“对象组管理”界面。

步骤6 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7 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。

警告

删除服务组后无法恢复，请谨慎操作。

----结束

8 拦截恶意攻击

8.1 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**。
- 开启私网IP流量防护请参见**开启NAT网关流量防护**。

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8-1**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 8-1 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。	• 检查威胁及漏洞扫描； • 检测流量中是否含有网络钓鱼、特洛伊木马、蠕虫、黑客工具、间谍软件、密码攻击、漏洞攻击、SQL注入攻击、XSS跨站脚本攻击、Web攻击； • 是否存在协议异常、缓冲区溢出、访问控制、可疑DNS活动及其它可疑行为。	查看和修改规则库请参见**修改入侵防御规则的防护动作**
虚拟补丁	在网络层级为IPS提供热补丁，实时拦截高危漏洞的远程攻击行为，同时避免修复漏洞时造成业务中断。 更新的规则优先进入虚拟补丁库中，您可以根据业务情况判断是否增加至基础防御库中。 增加方式：打开开关，虚拟补丁中的规则将生效，实时防护并支持手动修改防护动作。		
自定义IPS特征（仅专业版支持）	提供的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**自定义IPS特征**

- 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

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

8.2 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入“入侵防御”界面，保持“基础防御”右侧开关开启。

步骤6 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入“入侵防御”界面，保持“基础防御”右侧开关开启。

步骤6 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，拦截当次会话。
  - 拦截IP：发现敏感目录扫描攻击后，CFW会阻断该攻击IP一段时间。

    说明

    配置“拦截IP”后，CFW会持续对IP进行阻断，如果涉及地址转换或者存在代理的场景，需要谨慎评估拦截IP的影响。
- “持续时长”：“动作”选择“拦截IP”时，可设置阻断时间，范围为60~3600s。
- “阈值”：对于单个敏感目录扫描频率达到设定的阈值后，CFW会采取相应“动作”。

----结束

开启反弹 Shell 检测防御

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入“入侵防御”界面，保持“基础防御”右侧开关开启。

步骤6 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，拦截当次会话。
  - 拦截IP：发现反弹shell攻击后，CFW会阻断该攻击IP一段时间。

    说明

    配置“拦截IP”后，CFW会持续对IP进行阻断，如果涉及地址转换或者存在代理的场景，需要谨慎评估拦截IP的影响。
- “持续时长”：“动作”选择“拦截IP”时，可设置阻断时间，范围为60~3600s。

- “模式”：
  - 低误报：防护粒度较粗，单次会话中攻击次数达到4次时触发观察或拦截，确保攻击处理没有误报。
  - 高检测：防护粒度精细，单次会话中攻击次数达到2次时触发观察或拦截，确保攻击能够及时被发现并处理。

----结束

后续操作

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

8.3 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“攻击防御 > 病毒防御”，进入“病毒防御”页面。

步骤6 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 单击管理控制台左上角的，选择区域。

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

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

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

8.4 通过安全看板查看攻击防御信息

您可通过安全看板快速查看攻击防御功能（IPS、反弹Shell、敏感目录扫描、病毒防御）的防护信息，及时调整IPS防护。

通过安全看板查看 IPS 防护信息

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的 ，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“攻击防御 > 安全看板”，进入“安全看板”页面。

步骤6 在页面上方，选择“互联网边界”或“VPC边界”页签。

步骤7 查看防火墙实例下防护规则的统计信息，您可以在下拉框中选择查询时间。

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

表 8-2 安全看板可视化统计参数说明

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

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

  说明

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

----结束

相关操作

详细日志信息请参见**攻击事件日志**。

8.5 IPS 规则管理

8.5.1 修改入侵防御规则的防护动作

基础防御规则库和虚拟补丁规则库中的规则，支持手动修改防护动作，修改后，该规则不受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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“攻击防御 > 入侵防御”，进入“入侵防御”界面，保持“基础防御”右侧开关开启。

步骤6 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7 （可选）如需查看某类规则的参数详情，可在上方筛选输入框中，选择对应条件，筛选相关参数。

步骤8 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。

图 8-1 修改当前动作

说明

- 如果您当前页面无“操作”列，需返回上一层并开启“基础防御”右侧开关。
- 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”。

8.5.2 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，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6 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 8-3 添加自定义 IPS 特征

参数名称	参数说明
名称	需要添加的特征名称。 命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_）。 • 长度不能超过255个字符。
风险等级	设置特征的风险等级。
攻击类型	选择特征的攻击类型。
影响软件	选择受影响的软件。
操作系统	选择操作系统。
方向	选择该特征匹配流量的方向。 • Any：任意方向，符合其他条件的任意方向的流量都会匹配到当前规则。 • 服务器到客户端 • 客户端到服务器
协议类型	选择特征的协议类型。
源类型	选择源端口类型。 • Any：任意端口类型，等同于包含所有类型。 • 包含 • 排除 **说明** 建议您优先选择“Any”。
源端口	“源类型”选择“包含”或“排除”时，设置源端口。 • 支持设置单个或多个端口，多个端口之间用半角逗号（,）隔开，如：80,100。 • 支持连续端口组，中间使用“-”隔开，如：80-443。

参数名称	参数说明
目的类型	选择目的端口类型。 ● Any：任意端口类型，等同于包含所有类型。 ● 包含 ● 排除 **说明** 建议您优先选择“Any”。
目的端口	“目的类型”选择“包含”或“排除”时，设置目的端口。 ● 支持设置单个或多个端口，多个端口之间用半角逗号（,）隔开，如：80,100。 ● 支持连续端口组，中间使用“-”隔开，如：80-443。
动作	防火墙检测到该特征流量时，采取的动作。 ● 观察：仅对攻击事件进行检测并记录到日志中，日志记录查询请参见**日志查询**。 ● 拦截：实施自动拦截操作。 **说明** 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”。

参数名称	参数说明
内容	特征规则中匹配的内容。 ● 内容：跟特征匹配的内容字段，例如：cfw。 ● 内容选项：选择“内容”匹配的限制规则。 – 十六进制：匹配十六进制时，“内容”需填写十六进制格式，例如：0x1F。 – 忽略大小写：匹配时不区分大小写。 – URL：匹配URL中跟“内容”一致的字段。 ● 相对位置：匹配特征时，指定开始的位置。 – 头部：从报文“偏移”值的位置开始匹配特征，例如偏移：10，则该条内容从第11位开始。 **说明** 当“内容选项”选择“URL”时，头部的匹配位置从域名结束（包含端口）开始计算。 例如：www.example.com/test，偏移为0，则该条内容从com后的/开始。 或www.example.com:80/test，偏移为0，则该条内容从80后的/开始。 – 上一个内容之后：报文中截取的位置从指定位置开始。公式：上一条“内容”字段长度+上一条“偏移”值+“偏移”值+1 例如：上一条设置内容：test，偏移：10，本条偏移：5，则该条内容的匹配位置从第20（4+10+5+1）位开始。 ● 偏移：匹配特征时开始的位置，例如偏移：10，则代表该条内容的匹配位置从第11位开始。 ● 深度：匹配特征时，截止匹配的位置，例如深度：65535 ，则代表该条内容的匹配位置到第65535位截止。 **说明** ● “深度”值需大于“内容”字段长度。 ● 一条IPS特征中最多添加4条内容。

步骤7 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

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

9 查看流量数据

9.1 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“流量分析 > 入云流量”，进入“入云流量”页面。

步骤6 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。

  图 9-1 入云流量-流量看板

- 入云流量：入方向请求流量和响应流量数据，最多支持同时查询30个EIP的流量数据。

  数据信息是**流量日志**中在该时间结束会话的流字节数的平均值。

图 9-2 入云流量

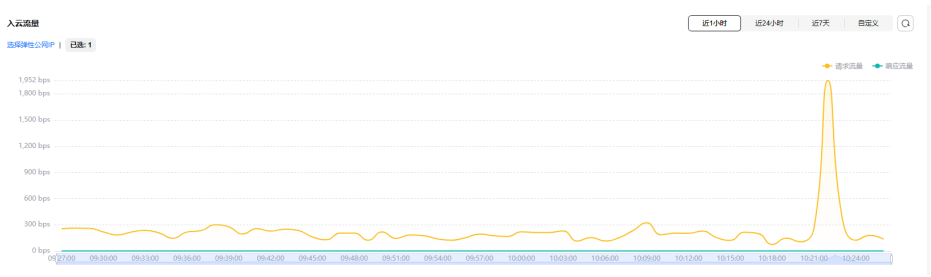


表 9-1 取值说明

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
自定义	- 5分钟~6小时：取1分钟内的平均值 - 6小时（含）~3天：取5分钟内的平均值 - 3天（含）~7天（含）：取30分钟内的平均值

- 可视化统计：查看指定时间段内入方向流量中指定参数的 TOP 5 排行，参数说明请参见表9-2。单击单条数据查看流量详情，每个详情支持查看50条数据。

图 9-3 入云流量-可视化统计

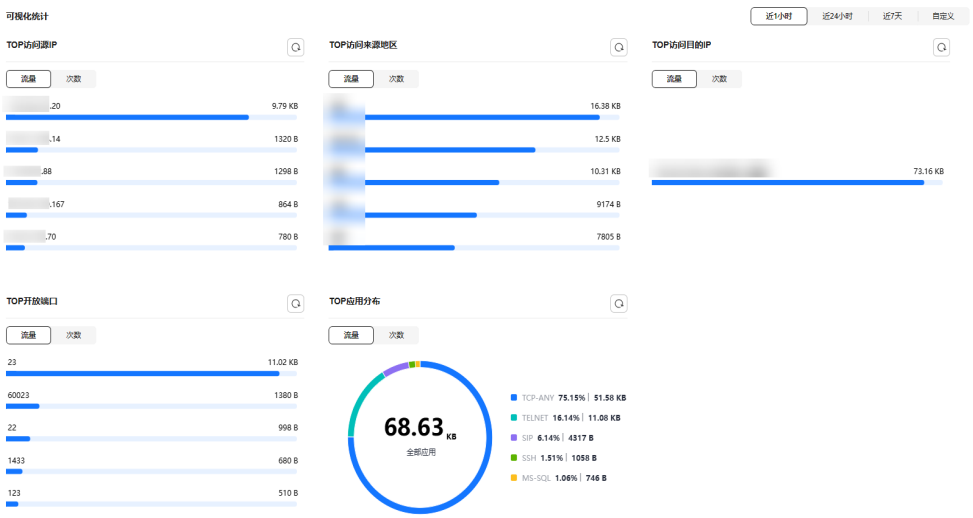


表 9-2 入云流量可视化统计参数说明

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，

参数名称	参数说明
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。

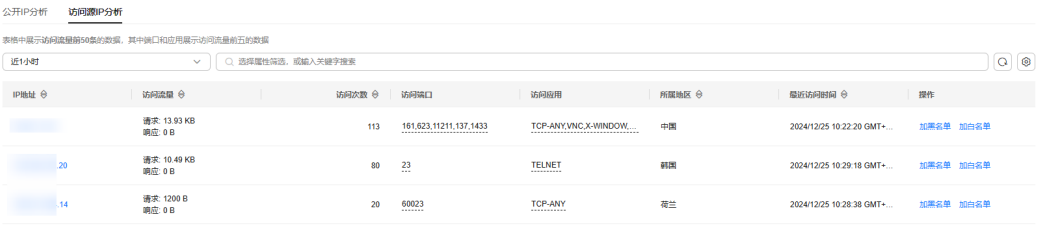
- IP分析：查看指定时间段内 TOP 50 的流量信息。
  - 公开IP分析：目的IP的流量信息。

    图 9-4 公开 IP 分析

  - 访问源IP分析：源IP的流量信息。

    图 9-5 访问源 IP 分析

----结束

9.2 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**。

规格限制

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

查看出云流量

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“流量分析 > 出云流量”，进入“出云流量”页面。

步骤6 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。

  图 9-6 出云流量-流量看板

- 出云流量：出方向请求流量和响应流量数据，最多支持同时查询30个EIP的流量数据。

  数据信息是**流量日志**中在该时间结束会话的流字节数的平均值。

  图 9-7 出云流量

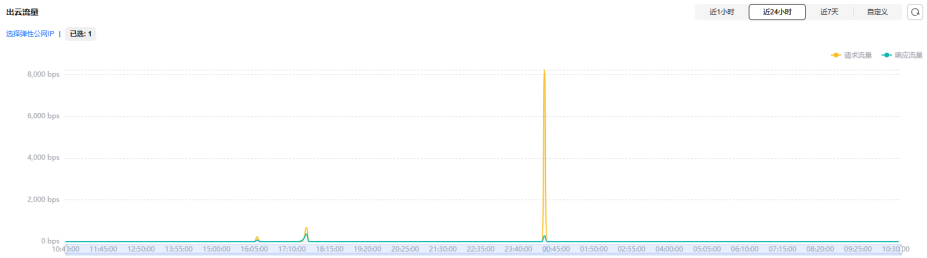
  

  表 9-3 取值说明

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
自定义	– 5分钟~6小时：取1分钟内的平均值 – 6小时（含）~3天：取5分钟内的平均值 – 3天（含）~7天（含）：取30分钟内的平均值

- 可视化统计：查看指定时间段内出方向流量中指定参数的 TOP 5 排行，参数说明请参见**表9-4**。单击单条数据查看流量详情，每个详情支持查看50条数据。

图 9-8 出云流量-可视化统计

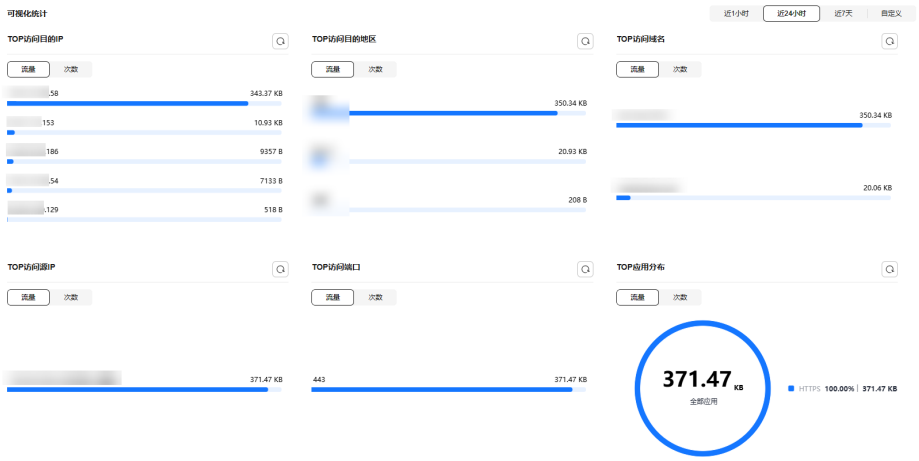
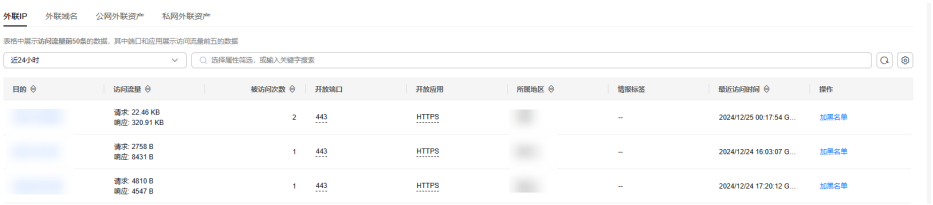


表 9-4 出云流量可视化统计参数说明

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。
TOP应用分布	出方向流量的应用信息。

- IP分析：查看指定时间段内 TOP 50 的流量信息。
  - 外联IP：目的IP的流量信息。

    图 9-9 外联 IP

  - 外联域名：域名信息。

    图 9-10 外联域名

  - 公网外联资产：源IP为公网IP的流量信息。

图 9-11 公网外联资产

- 私网外联资产：源IP为私网IP的流量信息。

图 9-12 私网外联资产

说明

私网IP信息仅配置了VPC边界防护的专业版防火墙可见。

----结束

9.3 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“流量分析 > VPC间访问”，进入“VPC间访问”页面。

步骤6 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。

图 9-13 VPC 间访问流量-流量看板

- VPC间访问：VPC间请求流量和响应流量数据。

数据信息是**流量日志**中在该时间结束会话的流字节数的平均值。

图 9-14 VPC 间访问

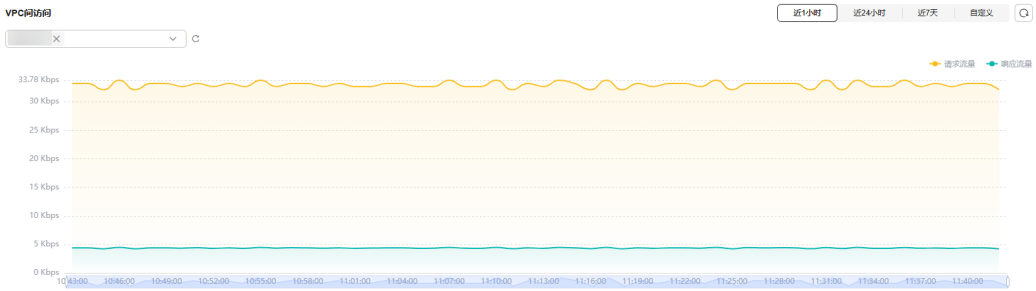


表 9-5 取值说明

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
自定义	- 5分钟~6小时：取1分钟内的平均值 - 6小时（含）~3天：取5分钟内的平均值 - 3天（含）~7天（含）：取30分钟内的平均值

- 可视化统计：查看指定时间段内VPC间流量中指定参数的 TOP 5 排行，参数说明请参见**表9-6**。单击单条数据查看流量详情，每个详情支持查看50条数据。

图 9-15 VPC 间访问流量-可视化统计

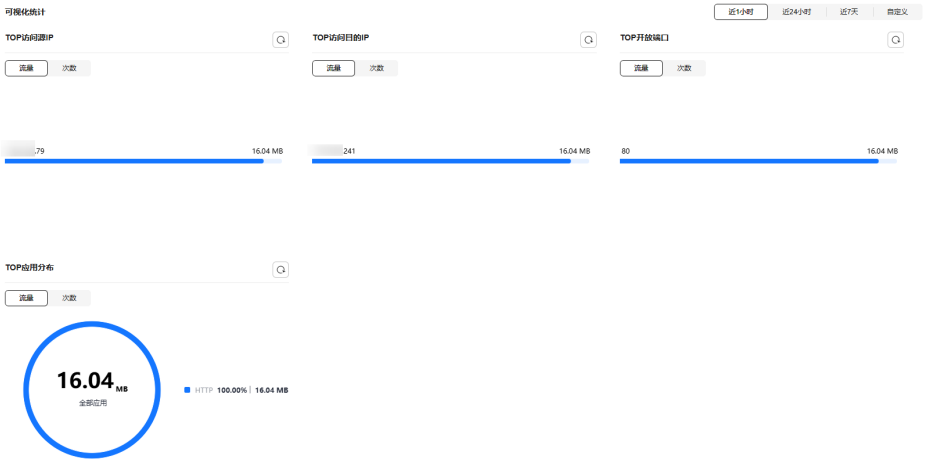


表 9-6 VPC 间流量可视化统计参数说明

参数名称	参数说明
TOP访问源IP	VPC间流量的源IP地址。

参数名称	参数说明
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。

  图 9-16 私网 IP 活动明细

----结束

10 查看云防火墙防护日志

10.1 防护日志概述

本文介绍以下内容：

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

日志存储方式

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

日志类型

提供以下日志：

- 攻击事件日志：IPS等攻击防御功能检测到的事件记录，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。

异常拦截排查

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

日志管理使用方式

功能名称	功能描述	配置方式
配置日志	将日志对接LTS，并创建日志组和日志流。	**配置日志**
更改存储时长	（可选）默认存储日志的时间为7天，存储时间可以在1～365天之间进行设置。	**更改日志存储时长**
日志搜索与分析	（可选）通过合理的日志收集、高效的搜索方法和专业的分析工具，实现对系统或应用的全面监控和精细化管理。	请参见**日志搜索与分析**
日志可视化	（可选）将日志数据按照图表类型呈现。	请参见**日志可视化**
配置告警规则	（可选）监控日志中的关键词，通过在一定时间段内，统计日志中关键字出现的次数，实时监控服务运行状态。	请参见**日志告警**
日志字段查看	介绍日志的中各个字段代表的含义。	**日志字段说明**

相关文档

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

10.2 日志查询

云防火墙支持查询7天内的日志记录，为您提供三类日志：

- 攻击事件日志：IPS等攻击防御功能检测到的事件记录，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。

说明

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

约束条件

- 日志存储时长最多支持7天。
- 单类日志最多支持查看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。

查看日志

参考以下操作查看日志。

攻击事件日志

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航树中，选择“日志审计 > 日志查询”。进入“攻击事件日志”页面，可查看近一周的攻击事件详情。

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

图 10-1 攻击事件日志

表 10-1 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。
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。

参数	说明
规则ID	对应规则的ID号。
规则名称	规则库中相对应的命中规则名称。
源IP	攻击事件的来源IP。 源IP为WAF回源IP时，“源IP”会展示WAF回源IP和RealIP，其中RealIP展示X-Forwarded-For对应的第一个IP，即客户端的真实IP。
标签	IP类型标识。 ● 其它标签：非WAF回源IP，无需特别处理。 ● WAF回源IP：“源IP”是WAF回源IP，如果本条记录的“响应动作”是阻断、阻断IP、丢弃，需手动设置放行。 操作方式：根据“规则ID”在IPS规则库中，在该规则的“操作”列，选择“观察”。
源国家/地区	攻击事件源IP所属的地理位置。
源端口	攻击事件的源端口。
目的IP	攻击事件中受到攻击的IP地址。
目的国家/地区	攻击事件目的IP所属的地理位置。
目的端口	攻击事件的目的端口。
协议	攻击事件的协议类型。
应用	攻击事件的应用类型。
方向	包括两个方向：出方向、入方向。
响应动作	防火墙的动作。 ● 放行 ● 阻断 ● 阻断IP ● 丢弃
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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航树中，选择“日志审计 > 日志查询”。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**。

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

图 10-2 访问控制日志

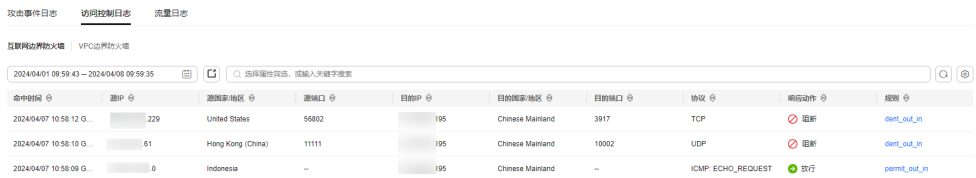


表 10-2 访问控制日志参数说明

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 单击管理控制台左上角的  ，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航树中，选择“日志审计 > 日志查询”，选择“流量日志”页签，可查看近一周的流量字节数和报文数。

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

图 10-3 流量日志

表 10-3 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。
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**。

10.3 日志管理

10.3.1 配置日志

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

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

须知

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

配置日志

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的  ，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航树中，选择“日志审计 > 日志管理”，进入“日志管理”页面。单击“LTS同步设置”，开启对接云日志服务  。

步骤6 创建日志组和日志流。操作步骤请参见**创建日志组和日志流**。

说明

为方便后续查看，建议您：

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

步骤7 选择已创建的日志组和日志流。选择日志组，开启并选择日志流，单击“确定”，完成日志配置。

说明

- 攻击、访问、流量日志的格式均不一样，需配置不同的日志流分别记录。
- 攻击日志：记录攻击告警信息，包括攻击事件类型、防护规则、防护动作、五元组、攻击payload等信息。

  访问日志：记录命中ACL策略的流量信息，包括命中时间、五元组、响应动作、访问控制规则等信息。

  流量日志：记录所有通过云防火墙的流量信息，包括开始时间、结束时间、五元组、字节数、报文数等信息。
- 配置完成后，如果出现“您的权限不足”的提示，请授予“LTS FullAccess”权限。

----结束

10.3.2 更改日志存储时长

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

更改日志存储时长

步骤1 将日志转储至LTS，操作步骤请参见**配置日志**。

步骤2 **登录管理控制台**。

步骤3 单击管理控制台左上角的  ，选择区域。

步骤4 在左侧导航栏中，单击左上方的  ，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

步骤5 （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6 在左侧导航树中，选择“日志审计 > 日志管理”，进入“日志管理”页面，单击“修改存储时长”。

说明

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

----结束

10.3.3 日志字段说明

本节介绍对接到LTS的日志字段。

攻击事件日志

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

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

访问控制日志

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

流量日志

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

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

11 系统管理

11.1 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。
- 异常外联告警：检测到外联风险IP或域名的可疑行为时触发告警。

说明

- 消息通知服务为付费服务，价格详情请参见**SMN价格详情**。
- 在设置告警通知前，建议您先在“消息通知服务”中创建“消息主题”，详细操作请参见**如何发布主题消息**。

设置告警通知

参考以下操作设置告警通知。

攻击告警

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 告警通知”，进入“告警通知”页面。

图 11-1 告警通知

步骤6 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。

图 11-2 通知项设置-攻击告警

表 11-1 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。
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。 单击“查看主题”创建新主题的操作步骤如下： 1. 参见**创建主题**创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。 3. 确认订阅。添加订阅后，完成订阅确认。

步骤7 单击“确认”，完成通知项设置。

步骤8 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 告警通知”，进入“告警通知”页面。

图 11-3 告警通知

步骤6 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。

图 11-4 通知项设置-流量超额预警

表 11-2 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。

参数名称	参数说明
通知等级	选择触发通知的流量等级，当流量（出流量或入流量的最大峰值）达到采购流量的该比例时，触发告警通知。 在下拉框中选择触发通知的流量占比等级，可选择“70%”、“80%”、“90%”。 例如：选择“80%”，那么当所用流量/购买流量=80%时，发送告警通知。
通知时间	选择通知的时间段。
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。 单击“查看主题”创建新主题的操作步骤如下： 1. 参见**创建主题**创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。 3. 确认订阅。添加订阅后，完成订阅确认。

步骤7 单击“确认”，完成通知项设置。

步骤8 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 告警通知”，进入“告警通知”页面。

图 11-5 告警通知

步骤6 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。

图 11-6 通知项设置-EIP 未防护告警

表 11-3 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。 单击“查看主题”创建新主题的操作步骤如下： 1. 参见**创建主题**创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。 3. 确认订阅。添加订阅后，完成订阅确认。

步骤7 单击“确认”，完成通知项设置。

步骤8 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

异常外联告警

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 告警通知”，进入“告警通知”页面。

图 11-7 告警通知

步骤6 在“异常外联告警”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。

图 11-8 通知项设置-异常外联告警

表 11-4 异常外联告警参数说明

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	设置触发条件。 **说明** 在设置时间间隔内，当异常外联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。 单击“查看主题”创建新主题的操作步骤如下： 1. 参见**创建主题**创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。 3. 确认订阅。添加订阅后，完成订阅确认。

步骤7 单击“确认”，完成通知项设置。

步骤8 确认信息无误后，在“异常外联告警”所在行的“生效状态”列，单击 ，开启异常外联通知。

----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。

11.2 网络抓包

11.2.1 新建抓包任务检查网络状态

当您需要定位网络故障和攻击时，参考本文创建网络抓包任务。

规格限制

仅专业版防火墙支持网络抓包功能。

约束条件

- 仅支持同时运行1个抓包任务。
- 每日限制创建20个抓包任务。
- 抓包数最大支持一百万个。

新建抓包任务检查网络状态

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 网络抓包”，进入“网络抓包”页面。

步骤6 单击“新建抓包任务”，在“新建抓包任务”中，填写参数如表 新建抓包任务所示。

表 11-5 新建抓包任务

参数名称	参数说明	取值样例
任务名称	自定义抓包任务名称。 命名规则如下： • 可输入中文字符（占用3个字符）、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_）。 • 长度不能超过30个字符。	cfw
最大抓包数	设置最大抓包数。支持输入1~1,000,000之间的整数。	100000

参数名称	参数说明	取值样例
抓包时长（分钟）	设置抓包的最长时间。支持输入1~10分钟之间的整数。	3
IP类型	设置抓包的IP类型，默认IPv4。	IPv4
协议类型	选择抓包的协议类型。支持选择以下协议： ● Any ● TCP ● UDP ● ICMP	Any
源地址	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
源端口	（可选）设置源端口。 输入规则如下： ● 为空时代表所有端口号（1-65535）。 ● 支持1-65535范围内的单个端口号。	80
目的地址	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
目的端口	（可选）设置目的端口。 输入规则如下： ● 为空时代表所有端口号（1-65535）。 ● 支持1-65535范围内的单个端口号。	-

步骤7 单击“确认”，完成抓包任务的创建。

----结束

相关操作

- 复制任务信息：在目标任务所在行的“操作”列中，单击“复制”，在“新建抓包任务”填写“任务名称”后，单击“确认”，可以快速复制抓包任务。

- 截止抓包任务：在目标任务所在行的“操作”列中，单击“截止”，可以截止抓包任务。
- 删除抓包任务：勾选目标任务，单击列表上方的“删除”，可以批量删除抓包任务。
- 查看抓包任务
- 下载抓包结果

11.2.2 查看抓包任务

查看抓包任务

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 网络抓包”，进入“网络抓包”页面。

步骤6 （可选）当任务较多时，可以通过搜索功能，选择“任务名称”或“IP地址”，并在搜索框中输入关键词，单击，即可快速查询指定任务。

- 任务名称：支持模糊搜索。输入规则如下：
  - 可输入中文字符（占用3个字符）、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_）。
  - 长度不能超过30个字符。
- IP地址：支持输入单个且完整的IP地址，例如0.0.0.0。

步骤7 查看抓包任务信息，参数说明如表 抓包任务参数说明所示。

表 11-6 抓包任务参数说明

参数名称	参数说明
任务名称	抓包任务的名称。
状态	当前任务的状态。 • 执行中：抓包命令已下发，任务进行中。 • 已完成：抓包结果上传完毕，任务已完成。 • 异常：网络原因导致抓包数据上传超时，抓包结果部分缺失。 **说明** 您可单击“操作”列中的“复制”，新建一个抓包任务重新执行。 • 截止中：截止命令已下发，抓包结果上传中。 • 已截止：抓包结果上传完毕，任务已提前结束。

参数名称	参数说明
协议类型	抓包的协议类型。
IP地址	抓包的IP地址，包括“源地址”和“目的地址”。
端口	抓包的端口，包括“源端口”和“目的端口”。
最大抓包数	当前任务的最大抓包数。
抓包时间	抓包任务运行的起止时间。
抓包时长（分钟）	抓包的运行时长。
剩余保留天数	抓包任务的保留天数，默认7天。
容量	抓包数据的大小。

----结束

相关操作

- 复制任务信息：在目标任务所在行的“操作”列中，单击“复制”，在“新建抓包任务”填写“任务名称”后，单击“确认”，可以快速复制抓包任务。
- 截止抓包任务：在目标任务所在行的“操作”列中，单击“截止”，可以截止抓包任务。
- 删除抓包任务：勾选目标任务，单击列表上方的“删除”，可以批量删除抓包任务。
- **新建抓包任务检查网络状态**
- **下载抓包结果**

11.2.3 下载抓包结果

限制说明

“状态”为“异常”的任务，抓包结果存在两种情况：

- 抓包数据完全缺失，无法下载。
- 抓包数据部分缺失，已有数据支持下载。

下载抓包结果

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 网络抓包”，进入“网络抓包”页面。

步骤6 在目标任务所在行的“操作”列中，单击“下载”，查看“抓包结果下载”。

说明

“状态”为“异常”的任务，抓包结果存在两种情况：

- 抓包数据完全缺失，无法下载。
- 抓包数据部分缺失，已有数据支持下载。

步骤7 抓包结果分享或下载，根据需求选择“抓包结果下载范围”。

说明

分享链接生成后三十分钟内有效，请及时使用或重新生成。

- 无限制：任意人员都可以通过链接下载抓包文件。
  - 抓包结果分享：单击右下角“复制全部”，将信息分享给他人。
  - 抓包结果下载：单击右下角“跳转”，前往浏览器中，单击“提取码”侧的“复制”，粘贴至“提取码”中，单击“获取分享目录列表”。
- 指定公网IP可用：设置允许下载抓包结果的地址段；仅支持该地址段通过本次生成的链接下载抓包结果。

  设置完成后单击“生成链接”，抓包结果的所有文件将展示在下方列表中。
  - 单个/多个抓包结果分享：单击列表中“下载链接”列的“复制链接”，将信息分享给他人。

    对方收到信息后，将链接信息粘贴至浏览器中，可直接下载抓包结果文件。
  - 抓包结果下载：
    - 下载单个结果：单击列表中“下载链接”列的“下载”，获取单个结果文件。
    - 下载全部结果：单击右下角“下载全部”，获取全部结果文件。

图 11-9 抓包结果下载

说明

- 单次设置最大支持添加三个地址段。
- “抓包结果下载”页面再次打开时，可重新设置地址段并生成新的链接信息。
- 如果您的IP地址不在设置的地址段内，您仍可以分享但无法下载抓包结果。

----结束

11.3 多账号防护

云防火墙服务具备安全可靠的跨账号数据汇聚和资源访问能力，如果您的账号由组织管理，您可以对组织内任意成员账号的EIP进行统一的资产防护。

约束限制

- 不支持跨区域防护EIP资源，如需在其它区域使用，请切换到对应区域购买防火墙，具体操作请参见**购买及变更云防火墙**。
- 单个防火墙实例支持防护的账号个数如下：
  - 包年/包月防火墙：
    - 标准版：20个
    - 专业版：50个
  - 按需计费防火墙（专业版）：20个

配置示例

通过CFW对组织成员账号进行资产防护需要执行以下操作（以A账号管理B账号下的资产为例）：

1. 如果A账号是组织管理员，则跳过此步骤。如果A账号不是组织管理员，则由组织管理员将A账号添加为委托管理员，相关操作请参见**添加委托管理员**。
2. 由A账号（组织管理员或委托管理员）邀请B账号加入组织，相关操作请参见**邀请账号加入组织**。
3. A账号在CFW中将B账号加入“多账号管理”页面的列表中，请参见**步骤5**。

有关组织的详细说明请参见**《组织用户指南》**。

说明

为了请求B账号下的EIP的信息，CFW会自动在A账号和B账号中创建服务关联委托：

- 该委托是云服务委托，委托权限为“CFWServiceLinkedAgencyPolicy”，“委托名称”为“ServiceLinkedAgencyForCloudFirewall”，授权范围为“所有资源”。
- 删除B账号时，CFW会自动删除B账号内的服务关联委托。
- 退订云防火墙服务时，CFW会自动删除A账号和所有成员账号内的服务关联委托。

添加组织成员账号

步骤1 （可选）开通企业中心，详情请参见：**开通企业中心功能**。

如果已开通企业中心，请跳过此步骤。

步骤2 （可选）开通组织服务并创建组织。

如果已开通组织服务，请跳过此步骤。

说明

如果已经加入组织，请退出已加入的组织后再进行创建组织操作，退出组织操作步骤请参见**成员账号退出组织**。

1. **登录管理控制台**。
2. 单击左上方的，选择“管理与监督 > 组织 Organizations”。
3. 开通Organizations云服务。进入开通页，单击“立即开通”。

图 11-10 开通 Organizations 云服务

开通Organizations云服务后，系统会自动创建组织和根组织单元，并将开通服务的账号设置为管理账号。

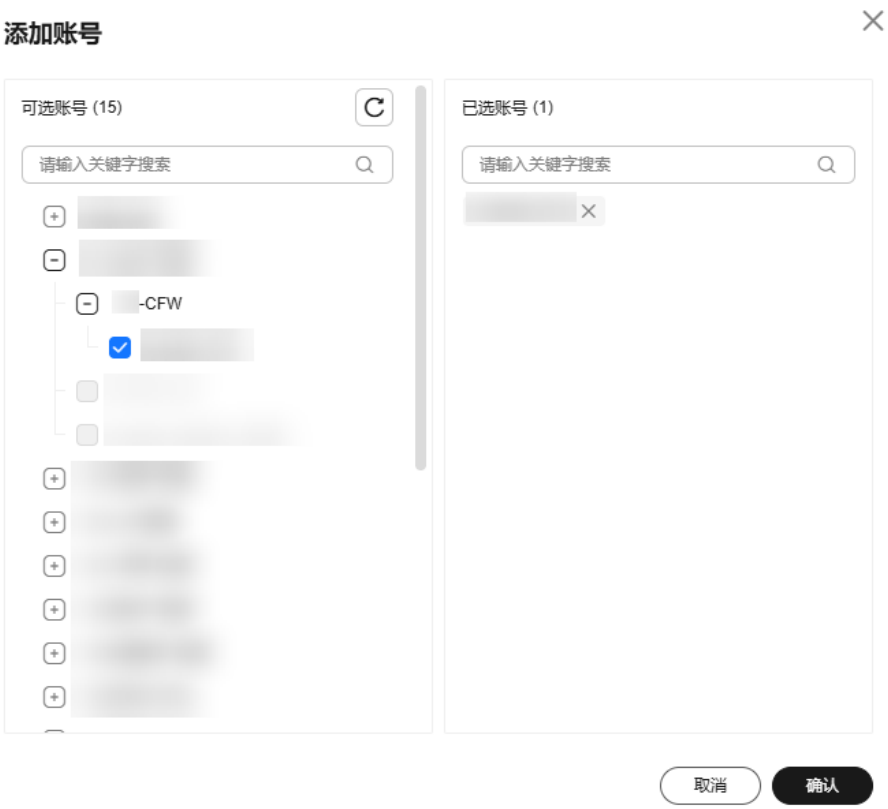
步骤3 设置CFW为可信服务，操作详情请参考**启用、禁用可信服务**。

步骤4 当前操作的账号为组织管理账号或委托管理员账号，添加委托管理员请参见**添加委托管理员**。

步骤5 添加组织成员账号。

1. 在左侧导航栏中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。
2. （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。
3. 在左侧导航栏中，选择“系统管理 > 多账号管理”，进入“多账号管理”页面。
4. 单击“添加账号”，弹出页面通过树状展开勾选目标账号，自动添加至右侧“已选账号”。

图 11-11 添加组织成员账号



说明

添加的账号需为同一个组织内的账号，有关组织账号的详细说明请参见《组织账号概述》。

5. 单击“确认”，在账号列表可查看添加的账号。
6. （可选）查看组织成员的EIP资源：
   a. 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。
   b. 单击右上角“资产同步”，将EIP资源信息同步至列表中。

----结束

查看组织成员账号

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 多账号管理”，进入“多账号管理”页面。

步骤6 查看全部账号列表信息。账号列表信息参数说明请参见**表 账号列表参数说明**。

表 11-7 账号列表参数说明

参数名称	参数说明
账号名	账号名称。
EIP数	账号下的EIP数量。
已开启防护数量	当前防火墙防护的EIP数量。
未开启防护数量	当前防火墙未开启防护的EIP数量。

----结束

相关操作

删除组织成员账号：勾选目标账号，单击列表上方的“删除账号”。

11.4 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > DNS配置”，进入“DNS配置”页面。

步骤6 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7 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

11.5 安全报告管理

11.5.1 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 安全报告”，进入“安全报告”页面。

步骤6 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 11-8 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。

参数名称	参数说明
报告类型	• 安全日报 统计周期：每天00:00:00 ~ 24:00:00 报告将在生成后的次日自动发送至您设置的报告接收人。 • 安全周报 统计周期：周一00:00:00 ~ 周日24:00:00 报告将在生成后的指定时间自动发送至您设置的报告接收人。 • 自定义报告：自定义选择时间范围。 统计周期：您可自定义安全报告统计的时间范围 报告将会在创建成功一段时间后生成，生成后会自动发送至您设置的报告接收人。
统计周期	“报告类型”选择“自定义报告”时，需要配置日志统计周期。
报告发送时间	当“报告类型”选择为“日报”、“周报”时，需要设置报告发送时间点，默认发送上一个统计周期的日志报告。 **说明** 为了保证正确性，报告发送时间可能存在延迟。
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。 单击“查看主题”创建新主题的操作步骤如下： 1. 参见**创建主题**创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。 3. 确认订阅。添加订阅后，完成订阅确认。

步骤7 单击“确认”，安全报告创建完成。

----结束

11.5.2 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 单击管理控制台左上角的  ，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 安全报告”，进入“安全报告”页面。

步骤6 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。

图 11-12 获取最新报告

步骤7 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 单击管理控制台左上角的，选择区域。

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

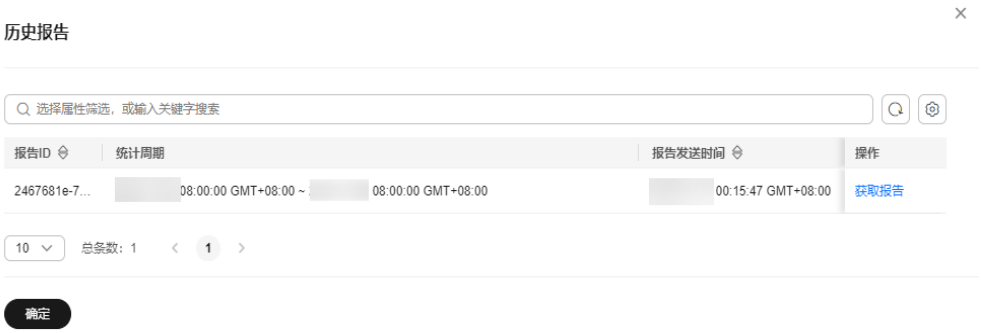
步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 安全报告”，进入“安全报告”页面。

步骤6 单击目标报告的“历史报告 ”，弹出“历史报告”，可查看报告列表。

图 11-13 获取历史报告

图 11-14 历史报告列表



步骤7 单击“操作”列的“获取报告”，可查看报告信息。

步骤8 如需下载，单击右下角的“下载”，可获取报告。

----结束

11.5.3 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 安全报告”，进入“安全报告”页面。

步骤6 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 单击管理控制台左上角的，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 安全报告”，进入“安全报告”页面。

步骤6 单击目标报告右下角的“编辑”，修改报告信息。

表 11-9 安全报告模板参数说明

参数名称	参数说明
报告名称	安全报告的名称。
报告类型	• 安全日报 统计周期：每天00:00:00 ~ 24:00:00 报告将在生成后的次日自动发送至您设置的报告接收人。 • 安全周报 统计周期：周一00:00:00 ~ 周日24:00:00 报告将在生成后的指定时间自动发送至您设置的报告接收人。
报告发送时间	当“报告类型”选择为“日报”、“周报”时，需要设置报告发送时间点，默认发送上一个统计周期的日志报告。
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。 单击“查看主题”创建新主题的操作步骤如下： 1. 参见**创建主题**创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。 3. 确认订阅。添加订阅后，完成订阅确认。

步骤7 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 单击管理控制台左上角的  ，选择区域。

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

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

步骤5 在左侧导航栏中，选择“系统管理 > 安全报告”，进入“安全报告”页面。

步骤6 单击目标报告右下角的“删除”，删除报告信息。

----结束

12 权限管理

12.1 CFW 自定义策略

如果系统预置的CFW权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**CFW权限及授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的CFW自定义策略样例。

CFW 自定义策略样例

- 示例1：授权用户创建云防火墙

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cfw:instance:create"
                                ]
        }
    ]
}
```

- 示例2：拒绝用户删除黑白名单

  拒绝策略需要同时配合其它策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予“CFW FullAccess”的系统策略，但不希望用户拥有“CFW FullAccess”中定义的删除黑白名单的权限（cfw:blackWhite:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后同时将“CFW FullAccess”和拒绝策略授予用户，根据Deny优先原则用户可以对CFW执行除了删除黑白名单的所有操作。以下策略样例表示：拒绝用户删除黑白名单。

```
{
    "Version": "1.1",
```



```
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "cfw:blackWhite:delete"
            ]
        },
    ]
}
```

- 多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其它服务的授权项，可以包含的其它服务必须跟本服务同属性，即都是项目级服务。多个授权语句策略描述如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cfw:instance:get",
                "cfw:eipStatistics:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "hss:hosts:switchVersion",
                "hss:hosts:manualDetect",
                "hss:manualDetectStatus:get"
            ]
        }
    ]
}
```

12.2 CFW 权限及授权项

如果您需要对您所拥有的CFW进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CFW服务的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是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。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

须知

请求峰值TPS大于2000TPS则要求本地鉴权。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

权限	授权项
创建云防火墙	cfw:instance:create
扩容云防火墙规格	cfw:instance:alterSpec
删除云防火墙	cfw:instance:delete
查询云防火墙	cfw:instance:get
查询云防火墙列表	cfw:instance:list
开启/关闭EIP防护	cfw:eip:operate
查询EIP列表	cfw:eip:list
查询EIP统计数据	cfw:eipStatistics:get
查询策略统计数据	cfw:policyStatistics:get
创建ACL规则	cfw:acl:create
修改ACL规则	cfw:acl:put
删除ACL规则	cfw:acl:delete
查询ACL规则列表	cfw:acl:list
设置ACL规则优先级	cfw:acl:setPriority
创建黑白名单	cfw:blackWhite:create
修改黑白名单	cfw:blackWhite:put
删除黑白名单	cfw:blackWhite:delete
查询黑白名单列表	cfw:blackWhite:list
创建IP地址组	cfw:ipGroup:create
修改IP地址组	cfw:ipGroup:put
删除IP地址组	cfw:ipGroup:delete
查询IP地址组列表	cfw:ipGroup:list
查询IP地址组详情	cfw:ipGroup:get
添加IP地址组成员	cfw:ipMember:create
更新IP地址组成员	cfw:ipMember:put
删除IP地址组成员	cfw:ipMember:delete
查询IP地址组成员列表	cfw:ipMember:list
创建服务组	cfw:serviceGroup:create

权限	授权项
修改服务组	cfw:serviceGroup:put
删除服务组	cfw:serviceGroup:delete
查询服务组详情	cfw:serviceGroup:get
查询服务组列表	cfw:serviceGroup:list
添加服务组成员	cfw:serviceMember:create
更新服务组成员	cfw:serviceMember:put
删除服务组成员	cfw:serviceMember:delete
查询服务组成员列表	cfw:serviceMember:list
查询访问控制日志列表	cfw:accessControlLog:list
查询流量日志列表	cfw:flowLog:list
查询攻击日志列表	cfw:attackLog:list
查询流量日志报表	cfw:flowLogReport:get
查询访问控制日志报表	cfw:accessControlLogReport:get
查询访问控制日志报表	cfw:attackLogReport:get
基础防御开启	cfw:ips:start
基础防御关闭	cfw:ips:stop
基础防御状态查询	cfw:ipsStatus:get
IPS防护模式设置	cfw:ipsMode:operate
IPS防护模式查询	cfw:ipsMode:get
创建抓包任务	cfw:captureTask:create
查询抓包任务列表	cfw:captureTask:list
批量删除抓包任务	cfw:captureTask:delete
停止抓包任务	cfw:captureTask:stop
下载抓包结果	cfw:captureTask:getResult
查询云防火墙实例资源	cfw:resource:list

13 使用 CES 监控 CFW

13.1 CFW 监控指标说明

功能说明

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

命名空间

SYS.CFW

说明

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

监控指标

表13-1是旧版指标，建议优先使用表13-2中指标。

表 13-1 云防火墙服务支持的监控指标（不建议使用）

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
used_protection_bandwidth	防护带宽使用量	该指标用于统计近5分钟内CFW检测到的互联网带宽使用量。 单位：KB/s	≥ 0 值类型：Float	云防火墙	5分钟

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

表 13-2 云防火墙服务支持的监控指标

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

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

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
internet_protection_bandwidth_usage_rate_outbound	出网防护带宽使用率	该指标为防火墙互联网防护对象带宽出方向使用率。 单位：%	≥ 0 值类型：Float	云防火墙	每分钟
internet_protection_pps_inbound	入网pps	该指标为访问防火墙互联网防护对象pps 单位：个	≥ 0 值类型：Float	云防火墙	每分钟
internet_protection_pps_outbound	出网pps	该指标为防火墙互联网防护对象访问外网pps 单位：个	≥ 0 值类型：Float	云防火墙	每分钟

维度

Key	Value
fw_instance_id	防火墙ID

13.2 设置监控告警规则

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

设置监控告警规则

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 ”。

步骤4 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤6 根据界面提示配置参数，关键参数如下，更多参数信息请参见创建告警规则和通知：

- 告警类型：指标
- 资源类型：云防火墙
- 维度：云防火墙实例

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

13.3 查看监控指标

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

查看监控指标

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

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

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

----结束

14 使用 CTS 审计 CFW 操作事件

14.1 支持云审计的 CFW 操作列表

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

云审计服务支持的CFW操作列表如**表 云审计服务支持的CFW操作列表**所示。

表 14-1 云审计服务支持的 CFW 操作列表

操作名称	资源类型	事件名称
EIP防护操作	cfw	eipOperateProtectService
EIP防护开启	cfw	eipOperateProtectService Enable
EIP防护关闭	cfw	eipOperateProtectService Disable
创建ACL规则	acl	addRuleAclService
修改ACL规则	acl	updateRuleAclService
删除ACL规则	acl	deleteRuleAclService
设置ACL规则优先级	acl	setACLRulePriority
创建黑名单	black_white_list	addBlackListService
修改黑名单	black_white_list	updateBlackListService
删除黑名单	black_white_list	deleteBlackListService
创建白名单	black_white_list	addWhiteListService
修改白名单	black_white_list	updateWhiteListService
删除白名单	black_white_list	deleteWhiteListService

操作名称	资源类型	事件名称
新建IP地址组	address_group	addAddressSetInfoService
更新IP地址组	address_group	updateAddressSetInfoService
删除IP地址组	address_group	deleteAddressSetInfoService
添加IP地址组成员	address_group	addAddressItemsService
更新IP地址组成员	address_group	updateAddressItemService
删除地址组成员	address_group	deleteAddressItemService
新建服务组	service_group	addServiceSetService
更新服务组	service_group	updateServiceSetService
删除服务组	service_group	deleteServiceSetService
添加服务组成员	service_group	addServiceItemsService
更新服务组成员	service_group	updateServiceItemService
删除服务组成员	service_group	deleteServiceItemService
创建东西向防火墙	cfw_instance	createEWFirewallInstance
创建南北向防火墙	cfw_instance	createSNFirewallInstance
更新防火墙	cfw_instance	updateFirewallInstance
删除防火墙	cfw_instance	deleteFirewallInstance
升级防火墙	cfw_instance	upgradeFirewallInstance
新增标签	cfw_instance	createTags
删除标签	cfw_instance	deleteTags
冻结防火墙	cfw_instance	freezeFirewallInstance
更新攻击日志下发配置信息	alarm_config	updateAlarmConfig
更新用户的域名服务器配置情况	dns_server	updateDnsServer
创建东西向墙	cfw	createEastWestFirewall
东西向墙开启防护	cfw	enableEwFirewallProtect
东西向墙关闭防护	cfw	disableEwFirewallProtect

操作名称	资源类型	事件名称
购买防火墙	cfw	addFirewallOrder
删除防火墙任务	cfw	deleteFirewall
升级防火墙任务	cfw	changeFirewall
ips防护模式修改/创建	ips	createOrUpdateIpsMode
开启虚拟补丁	ips	enableVirtualPatches
关闭虚拟补丁	ips	disableVirtualPatches
创建日志管理	log_config	createLogConfig
修改日志管理	log_config	updateLogConfig
导入ACL	import	importCFW

14.2 查看审计日志

开启了云审计服务后，系统开始记录CFW资源的操作。云审计服务管理控制台保存最近7天的操作记录。

查看审计日志的详细操作请参见**查看审计事件**。

