防火墙管理

操作指南

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

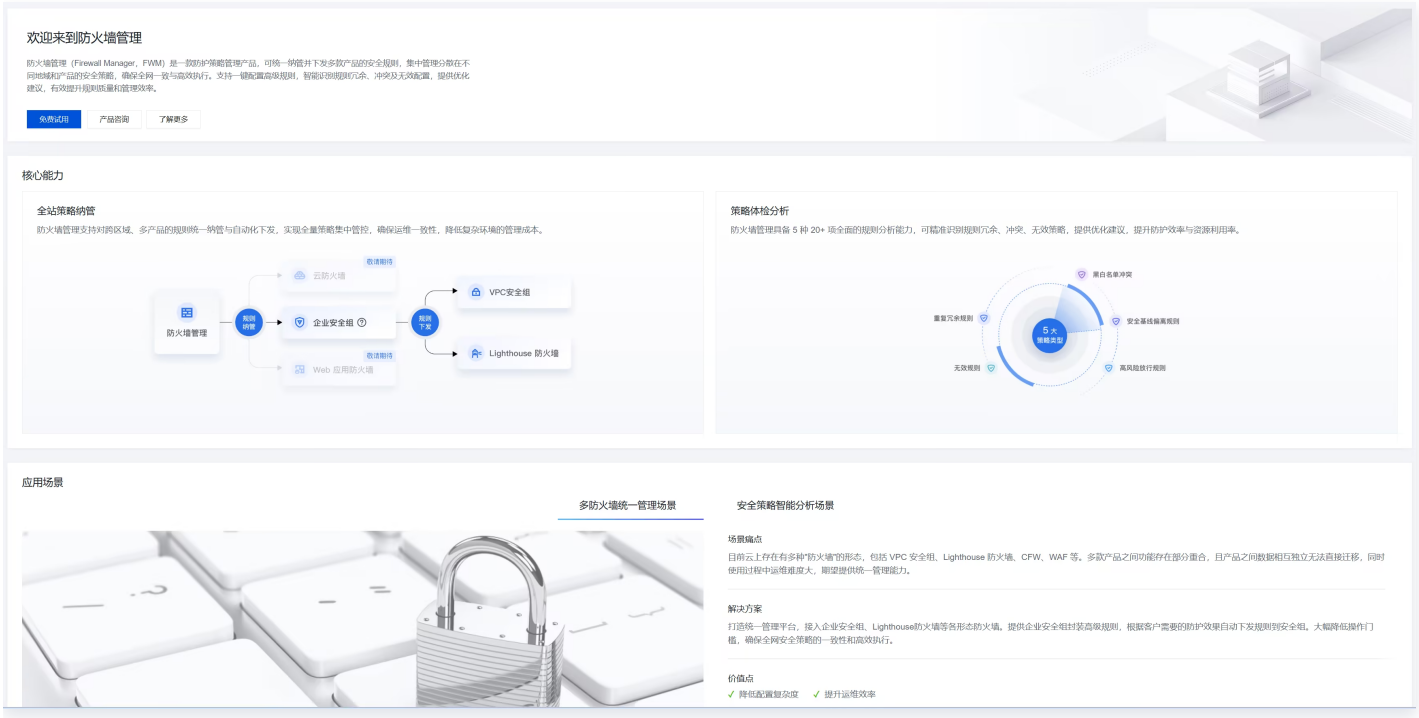
我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

操作指南
欢迎页

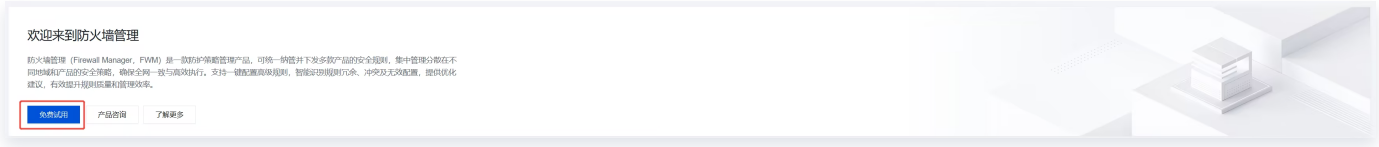
最近更新时间：2026-03-18 15:37:52

当您首次访问防火墙管理且未开通服务时，控制台将显示本欢迎页。
本页面旨在向您介绍防火墙管理的产品定位、核心价值与应用场景。您可在此页面一键申请免费试用，快速开启集中式安全策略管理体验。



操作步骤

1. 登录 防火墙管理 ，单击**免费试用**。



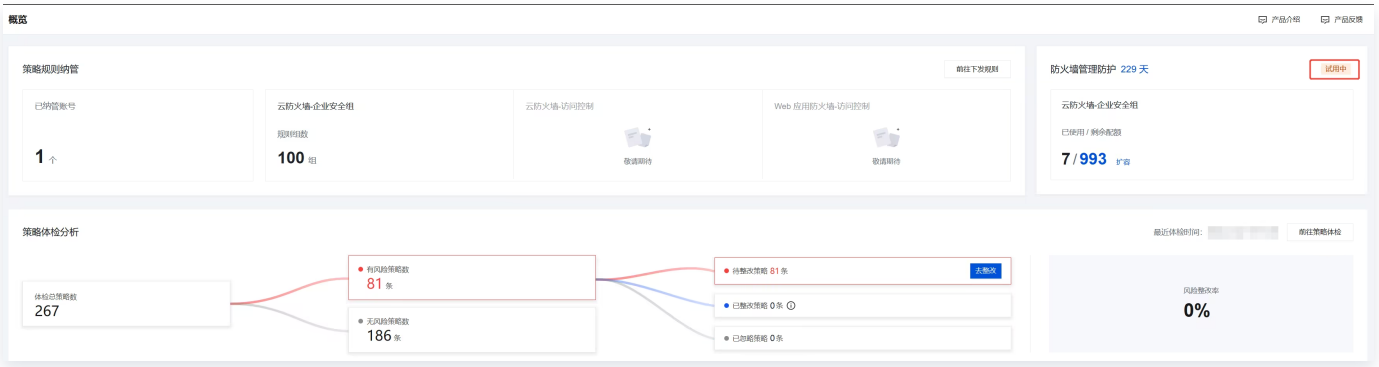
2. 在授权页面，单击**立即授权** > **同意授权**，完成腾讯云标准授权流程。

说明：

若用户已经使用了云防火墙的企业安全组，则不可使用防火墙管理。单击立即前往，跳转至 云防火墙 使用企业安全组。

3. 授权成功后，系统将自动跳转至防火墙管理的 概览 页面。

4. 在页面右上方，您将看到服务状态标识为**试用中**，表示您已成功开通免费试用，可以开始使用所有功能。



概览

最近更新时间：2026-03-18 15:37:52

功能简介

概览页面是防火墙管理的核心控制面板，为您集中展示账户的整体安全态势。您可在此快速查看策略规则纳管、防护状态、策略体检分析等关键信息，并执行相关快捷操作。

操作步骤

1. 登录 防火墙管理控制台 ，在左侧导航中，选择**概览**。
2. 在概览页面上方的策略规则纳管区域，您可以进行如下操作：
   - 查看当前已关联纳管的账号总数，以及各个安全产品下的规则组数量。

     > **说明：**
     > 当前仅支持云防火墙-企业安全组。

   - 单击**前往下发规则**，系统将跳转至**策略管理** > **规则下发管理** > **新建下发规则**页面，以便快速创建并下发安全规则。详情请参见 新建下发规则 。

3. 在概览页面右上方的防火墙管理防护区域，您可以进行如下操作：
   - 查看防火墙管理已防护天数，以及各安全产品已使用 / 剩余配额。
   - 单击**扩容**，可跳转至对应安全产品购买页面。

4. 在概览页面下方策略体检分析区域，您可以进行如下操作：
   - 查看上一次策略分析体检的执行完成时间，以及体检总策略数、有风险策略数、待整改策略、风险整改率等关键结果。
   - 单击待整改策略的**去整改**，跳转至策略分析界面，对发现的风险项进行处置。
   - 单击**前往策略体检**，将跳转至策略分析界面并自动弹出“开始体检”窗口，便于您立即发起一次新的策略健康检查。详情请参见 发起策略体检 。

策略管理
规则下发管理

最近更新时间：2026-03-18 15:37:52

功能简介

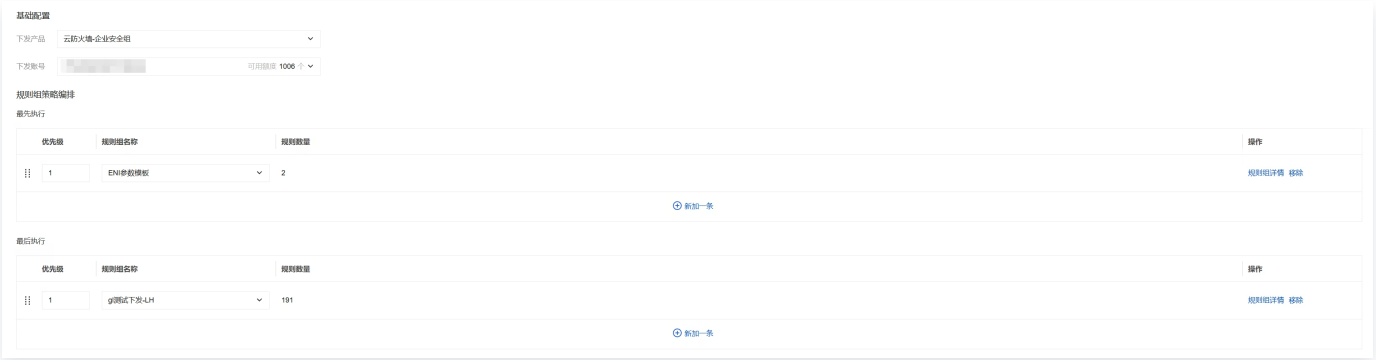
规则下发管理用于将规则组部署到指定的云产品与账号。您可在此页面，对支持的云安全产品的规则组进行下发、管理与监控。

操作步骤

1. 登录 防火墙管理控制台 ，在左侧导航中，选择**策略管理** > **规则下发管理**。
2. 单击**云防火墙-企业安全组**，切换到云防火墙-企业安全组界面。

新建下发规则

1. 在规则下发管理页面，单击**新建下发规则**。
2. 在新建下发规则页面，配置以下参数：



参数名称	说明
下发产品	选择 云防火墙-企业安全组。
下发账号	选择规则需要下发到的目标账号。
最先执行	配置优先级最高（最先执行）的规则组，单击**新加一条**以添加。
优先级	规则执行的先后顺序，数字越小优先级越高。仅首条规则的优先级可编辑，后续规则优先级自动递增。 **说明：** • 仅支持编辑首条规则的优先级，其后的规则会依次递增；原优先级所在的规则会自动递延。

	• 长按鼠标左键，即可拖动排序所创建的规则组策略，优先级也会随之变动。
规则组名称	从下拉列表中选择需要下发的规则组。 **说明：** 如现有规则组不符合您的要求，可单击**新建规则组**，系统将跳转至**策略管理 > 规则组管理 > 新建规则组**页面。具体操作请参阅 新建规则组 。
规则数量	（自动显示）所选规则组内包含的规则总数。
操作	• 规则组详情：查看该规则组的基础信息与规则列表。 • 移除：从当前编排中移除此规则组。
最后执行	配置优先级最低（最后执行）的规则组，单击**新加一条**以添加。参数说明同**规则组策略编排-最先执行**。

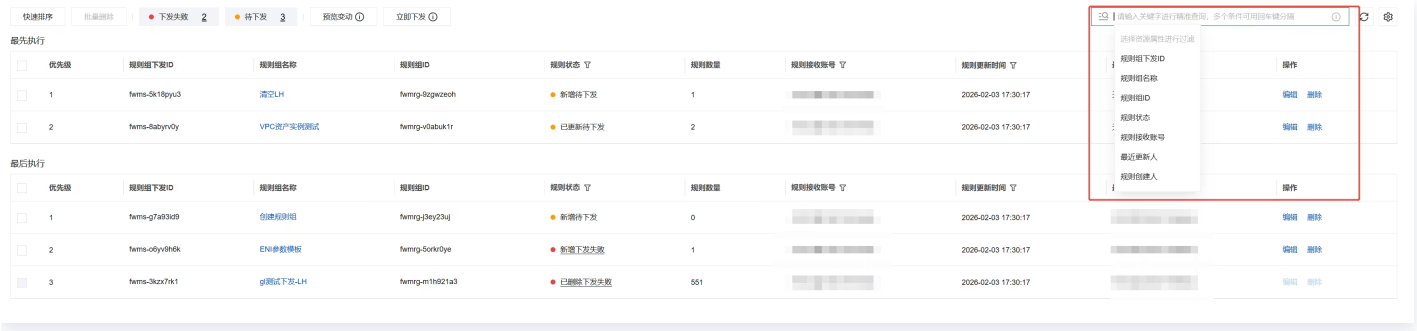
3. 参数配置完成后，您可以选择以下操作：
   - 保存并预览变动：保存下发规则组，并预览下发规则关联实例所绑定的安全组规则变动。
     - 确认无误后，单击**立即下发**可执行下发。
     - 也可单击**关闭**，系统将保存您的下发规则并返回规则下发管理页面。
   - 立即下发：下发此规则以及所有安全产品中所有的未下发、待下发以及下发失败规则。
   - 保存：保存至规则下发管理列表，后续需在规则下发管理列表中手动单击**立即下发**才会生效。

管理下发规则

在 规则下发管理 页面，您可以管理已创建的规则，进行查询、排序、下发、编辑和删除操作。

查询规则

您可以通过列表上方的搜索框，输入规则组下发ID、规则组名称等关键字进行查询，多个条件可用回车键分隔。



快速排序

规则在列表中的自上而下顺序代表其优先级从高到低。如需调整，请按以下步骤操作：

1. 单击列表上方的**快速排序**。
2. 将鼠标悬停在需调整的规则行上，光标变为拖动图标时，按住左键上下拖动。
3. 调整至目标位置后，单击**保存**。列表上方规则的优先级高于下方规则，系统会自动更新优先级数值。

下发规则

规则下发有两种主要方式：

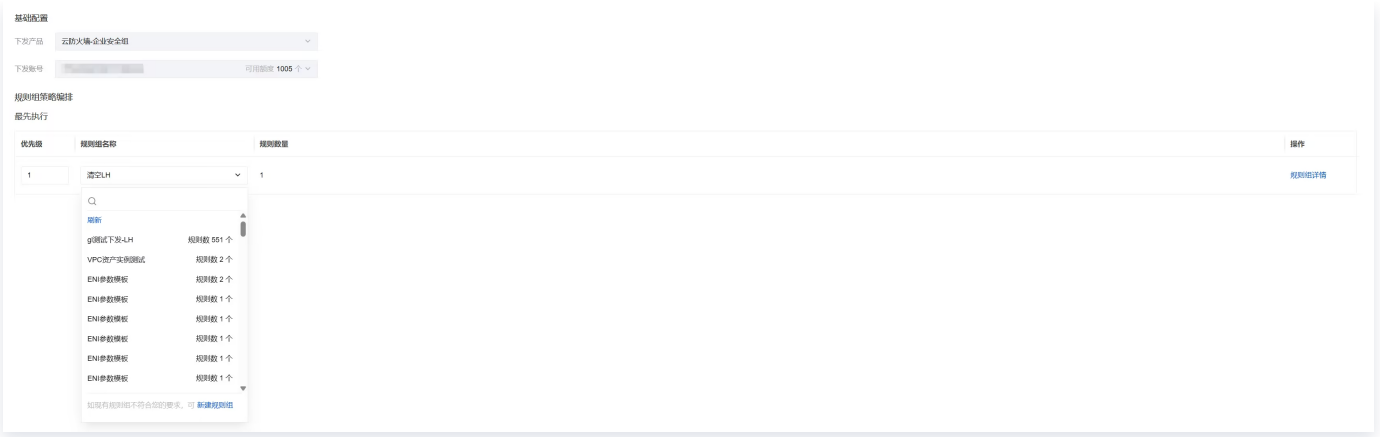
- 预览后下发：在新建、编辑下发规则时单击**保存并预览变动**，或在规则下发管理列表页面单击**预览变动**，将在新页面展示规则变更详情。确认无误后，单击该页面的**立即下发**。
- 直接下发：在新建、编辑下发规则时单击**立即下发**，或在规则下发管理列表页面单击**立即下发**，将直接触发下发流程。

> **注意：**
> 下发会将所有安全产品中所有的未下发、待下发以及下发失败规则进行下发。

编辑规则

1. 在目标规则的操作列中，单击**编辑**，进入编辑页面。

2. 在编辑页面，您可以修改“规则组策略编排”中的规则组优先级和规则组名称。



- 优先级：规则执行的先后顺序，数字越小优先级越高。仅首条规则的优先级可编辑，后续规则优先级自动递增。

  > **说明：**
  > - 仅支持编辑首条规则的优先级，其后的规则会依次递增；原优先级所在的规则会自动递延。
  > - 长按鼠标左键，即可拖动排序所创建的规则组策略，优先级也会随之变动。

- 规则组名称：从下拉列表中选择需要下发的规则组。

  > **说明：**
  > 如现有规则组不符合您的要求，可单击**新建规则组**，系统将跳转至**策略管理** > **规则组管理** > **新建规则组**页面。具体操作请参阅 新建规则组 。

- 单击**规则组详情**，可查看该规则组的基础信息与规则列表。

3. 参数配置完成后，您可以选择以下操作：
   - 保存并预览变动：保存下发规则组，并预览下发规则关联实例所绑定的安全组规则变动。
     - 确认无误后，单击**立即下发**可执行下发。
     - 也可单击**关闭**，系统将保存您的下发规则并返回规则下发管理页面。
   - 立即下发：下发此规则以及所有安全产品中所有的未下发、待下发以及下发失败规则。
   - 保存：保存至规则下发管理列表，后续需在规则下发管理列表中手动单击**立即下发**才会生效。

删除规则

- 单条删除：在目标规则的操作列中，单击**删除**。
- 批量删除：先勾选多个规则，再单击列表上方的**批量删除**。

注意：

删除后的规则无法恢复。

- **"新增待下发"状态规则会直接从列表移除。**
- **"已生效/已更新待下发"状态规则则会转为"已删除待下发"状态，需要单击立即下发才可生效。**

规则组管理

最近更新时间：2026-03-18 15:37:52

功能简介

规则组管理用于集中创建、编排和维护可复用的规则组。它支持对规则组及其内部规则进行全生命周期的精细化管控，包括新建、编辑、排序、筛选和批量操作，为后续的规则下发流程提供策略基础。

操作步骤

1. 登录 防火墙管理控制台 ，在左侧导航中，选择**策略管理 > 规则组管理**。
2. 单击**云防火墙-企业安全组**，切换到云防火墙-企业安全组界面。

新建规则组

1. 在规则组管理页面，单击**新建规则组**。
2. 在新建规则组页面，配置以下参数：

参数名称	说明
规则组名称	自定义规则名称，50个字符以内。
所属产品	选择云防火墙-企业安全组。
组内优先级	规则的执行顺序，企业安全组 IPv4和 IPv6规则的执行顺序互不影响，优先级较高的规则被优先匹配，命中后则不再匹配后序规则。当您修改某条规则的优先级时，原本该位置的规则的优先级+1，依次类推。当您删除某条规则时，后序所有规则的优先级-1。 **说明：**

	• 仅支持编辑首条规则的优先级，其后的规则会依次递增；原优先级所在的规则会自动递延。 • 长按鼠标左键，即可拖动排序所创建的规则组策略，优先级也会随之变动。
IP 类型	根据需求选择 IPv4 或者 IPv6。
访问源	• IPv4 规则支持 IP/CIDR、参数模板、资产实例、资源标签、资产地域等类型。 • IPv6 规则支持 IP/CIDR、参数模板等类型。
访问目的	• IPv4 规则支持 IP/CIDR、参数模板、资产实例、资源标签、资产地域、域名解析等类型。 • IPv6 规则支持 IP/CIDR、参数模板等类型。 **说明：** • 访问源选择其中的一种类型，访问目的也可以选择一种类型。但是，当访问源或访问目的选择的是资源地域时，对应的访问目的或访问源则不能选择资产地域，其他类型没有这个限制。 • 当生效范围选择轻量应用服务器防火墙时，访问源与访问目的均不支持参数模板类型。
目的端口	• 手动填写：支持单端口号、基于'/'的端口段以及英文逗号分隔的离散端口值、最多填写15个离散端口，例如“80”、“80/80”、“-1/-1”、“1/65535”。 • 参数模板：在已有端口模板协议内容中选择所需的地址模板。自定义端口协议模板可参考 地址模板 > **新增模板**。
协议	当前版本支持 UDP、TCP 和 ICMP 协议。
生效范围	您可以选择下发规则至安全组或轻量应用服务器防火墙。
策略	• 允许：放通命中规则的流量。 • 拒绝：拦截命中规则的流量。
描述	用于描述规则，最多支持30个字符，支持通过##的方式对当前规则进行 TAG 标记，其中部分 TAG 支持特殊功能；当前版本支持的设定有#仅下发访问源#, #仅下发访问目的# **说明** 当访问目的地址填写为实例、子网、私有网络地址时，可通过自动双向下发，分配一条相同的入站规则。如果不想实现双向下发的效果，可通过在描述添加关键

> 字： #仅下发访问源#（仅对访问源下发安全组规则），#仅下发访问目的#（仅对访问目的下发安全组规则）。

3. 若已编辑完成前方规则，而后方待配置规则与前者相似，可通过使用复制功能快速生成新规则，随后根据实际需求调整细节即可。
   - 单击操作栏的  ，可在当前所选规则位置的下方新增一行规则，并自动复制当前规则的全部内容；
   - 单击下方的  ，可在规则列表的最底部新增一行规则，并自动复制列表中最后一条规则的内容。

> **说明**
> 一个规则组单次最多支持添加10条规则。

4. 确认无误后，单击**确定**完成配置。

> **说明：**
> - 配置规则需手动下发：创建规则后，请前往 规则下发管理 ，单击**立即下发**以使规则生效。
> - 基于 IP 配置的风险提示：在资产 IP 不重复的情况下，您可通过 IP 地址快捷配置安全组规则。但需注意：**若某 IP 绑定了多个实例，该 IP 的规则将对其下所有实例生效**。后续如因资产变更导致该 IP 对应了新的实例，此规则也将自动扩展至所有关联实例。

管理规则组

在 规则组管理 页面，您可以通过组合多种资源属性来筛选和查询规则组，然后对目标规则组进行管理。

删除规则组

- 单条删除：在目标规则组的操作列中，单击**删除**。
- 批量删除：先勾选多个规则组，再单击列表上方的**批量删除**。

> **注意：**
>
> - 规则组存在关联下发账号时无法删除。请前往 **规则下发管理** 页面，移除相关下发规则组以确保无关联下发账号后再进行删除操作。
> - 删除后的规则组无法恢复。

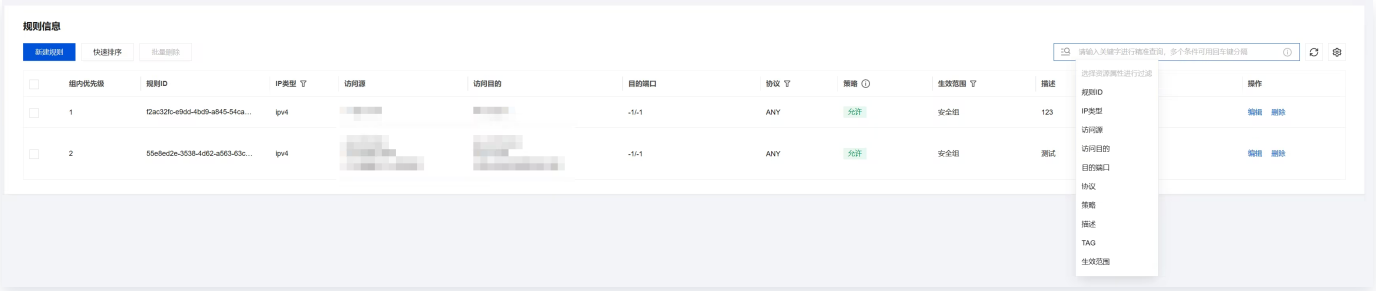
编辑规则组

在目标规则组的操作列中，单击**编辑**，可进入编辑页面。

该页面分为两部分：

- 基础信息：仅支持单击 修改规则组名称，其他基础信息参数不可编辑。

- 规则信息：支持对当前规则组内的所有规则进行新增、查询、修改、删除及排序等操作。



  - 查询规则：支持组合多种资源属性来筛选和查询规则。
  - 新建规则：单击**新建规则**，可在本组内新增一条规则，参数说明请参考 **新建规则组** 。
  - 编辑规则：单击目标规则操作列的**编辑**，可修改该规则的详细配置。

- 删除规则：单击目标规则操作列的**删除**，可删除该规则；勾选多个规则后，可单击**批量删除删除**多个规则。
- 快速排序：规则在列表中的自上而下顺序代表其优先级从高到低。如需调整，请按以下步骤操作：

  a. 单击列表上方的**快速排序**。

  b. 将鼠标悬停在需调整的规则行上，光标变为拖动图标时，按住左键上下拖动。

  c. 调整至目标位置后，单击**保存**。列表上方规则的优先级高于下方规则，系统会自动更新优先级数值。

策略分析

最近更新时间：2026-03-18 15:37:52

功能简介

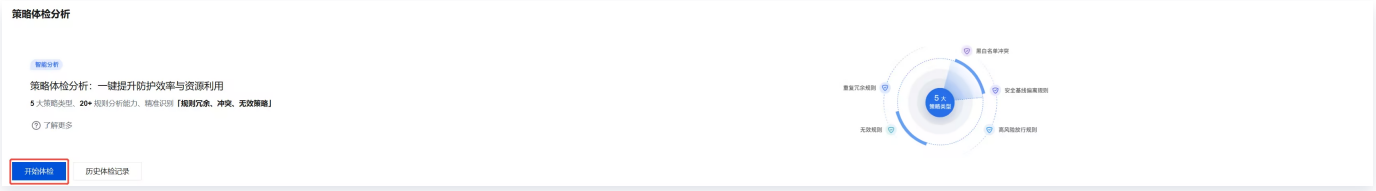
策略分析功能旨在对现有企业安全组及其内部的安全组规则进行深度分析。该功能通过展示风险分类、风险等级及规则分类等关键信息，辅助管理员精准识别可能存在的规则冗余、策略冲突及无效配置等问题。基于分析结果，系统会提供相应的优化建议，以帮助用户优化安全策略，从而提升产品的防护效率与资源利用率。

> **说明：**
> 本文档将以“企业安全组”为例，进行相关操作说明，“安全组”操作同理。

操作步骤

发起策略体检

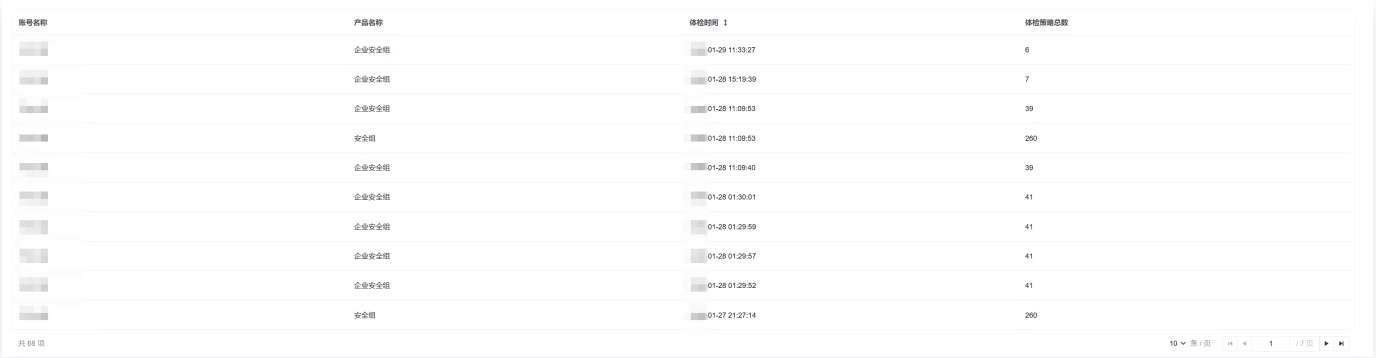
1. 登录 防火墙管理控制台，在左侧导航中，选择**策略管理** > **策略分析**，单击**开始体检**。



2. “体检产品”选择**企业安全组**，单击**开始体检**，即可对企业安全组策略进行体检。

3. 单击后，页面将显示“体检中”的加载状态，请耐心等待分析完成。

4. 您可以单击查看**历史体检记录**。历史记录按体检时间倒序排列，您可以查看任意一次历史体检的详细报告，其中包含该次体检时刻的策略风险快照。

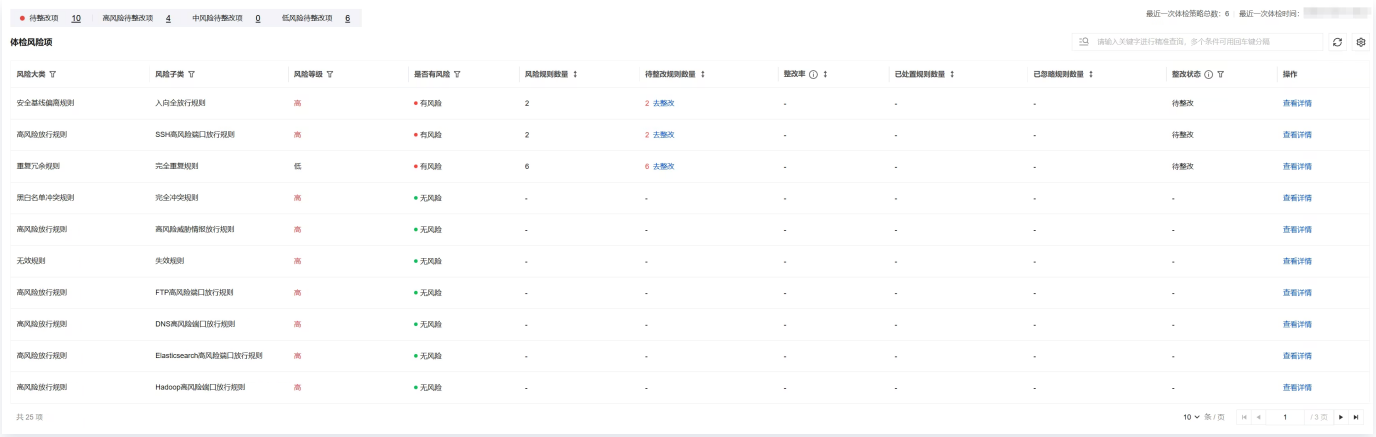


查看体检结果

分析完成后，页面默认展示最新一次的体检结果，包括：

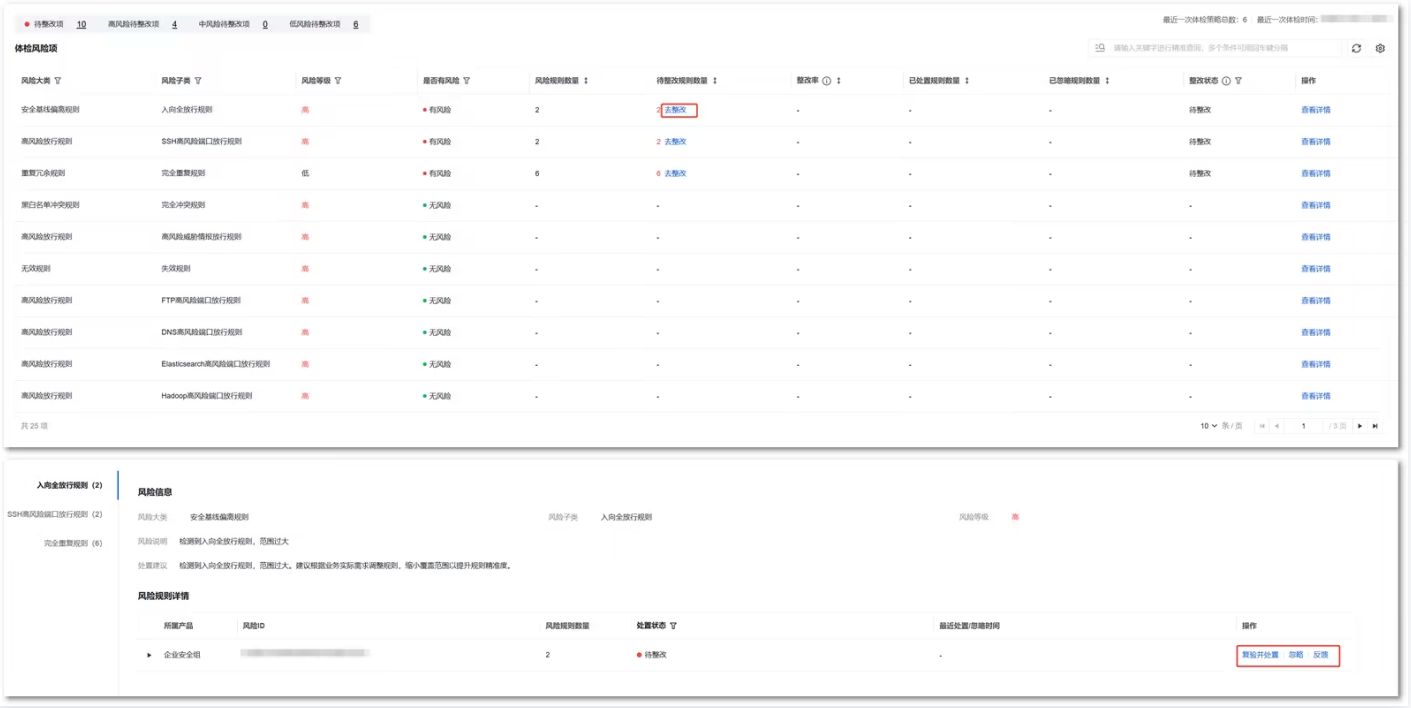
- 体检概览：展示该账号下所有受检产品（企业安全组+安全组）的综合风险概况。
  - 体检概览展示体检总策略数、有风险策略数、待整改策略、风险整改率等关键结果。
  - 风险整改率 = (已整改策略 + 已忽略策略) / 有风险策略数。

- 体检详情列表：
  - 列表默认按照风险严重程度与处置状态进行智能排序，确保有风险且待整改的策略优先展示。具体排序优先级为：高风险有待整改 > 中风险有待整改 > 低风险有待整改 > 高风险无待整改 > 中风险无待整改 > 低风险无待整改 > 高风险无风险 > 中风险无风险 > 低风险无风险。
  - 列表展示的字段包括：风险大类、风险子类、风险等级、风险策略数、待整改策略数、整改率、已处置策略数、已忽略策略数及整改状态。并支持对部分字段进行筛选与排序。
  - 整改率=（已处置+已忽略）/ 风险策略数。当整改率达到100%时，整改状态显示为“已整改”；小于100%时，显示为“待整改”；不涉及风险的条目则为“–”。
  - 关于体检风险项的说明，详情请参见 体检项说明 。



管理风险策略

对于识别出的风险策略，单击**去整改**，即可进入待整改风险项详情页面并管理风险策略。您可以进行复验并处置、忽略或误报反馈。



- **复验并处置**

  由于安全组规则没有唯一 ID，无法直接定位历史快照中的具体规则，因此每次处置前系统会重新进行实时检测，以确保操作的准确性。

  1.1 单击**复验并处置**后，系统弹窗并立即执行实时分析。

  - 若实时分析后无风险，则提示“暂无风险策略”，流程结束。
  - 若实时分析后存在风险策略，则会展示最新的风险规则列表（此列表可能与体检详情中的历史快照不一致，属于正常现象）。

  1.2 您可以在列表中直接对风险规则进行编辑或删除操作。

  1.3 处置循环：每完成一条风险的复验并处置，系统会再次触发实时检测。如果仍有风险，则继续展示并供您处置，直至所有风险被消除，系统提示“整改已完成”。

1.4 处置完成后，该条目的“复验并处置”将变为不可单击状态。

- **忽略**
  - 对于确认为误报或无需处置的风险，您可以单击**忽略**。忽略后，该风险在后续检测中仍会显示，但会被标记为“已忽略”。
  - 忽略后可以取消忽略。
- **反馈**：如果您认为某条风险策略属于误报，可以单击**反馈**，输入您的自定义说明（3000字以内）。您的反馈将用于持续优化内置的风险检测逻辑。

附录

体检项说明

风险大类	风险子类	风险等级	风险描述	处置建议
黑白名单冲突规则	完全冲突规则	高	检测到黑白名单五元组完全一致。	建议基于业务实际需求，仅保留一个规则，删除其余冲突规则。
安全基线偏离规则	入向全放行规则	高	检测到入向全放行规则，范围过大。	建议根据业务实际需求调整规则，缩小覆盖范围以提升规则精准度。
重复冗余规则	完全重复规则	低	检测到规则五元组与匹配动作完全一致。	建议仅保留一个规则，删除其余冗余规则。
	可合并规则	低	检测到规则的 IP/CIDR 连续端口一致 或 IP/CIDR 一致端口不一致。	建议将多规则合并至一条规则。
	部分重复规则	中	检测到规则五元组相同但匹配动作不同。	建议基于业务实际需求，仅保留一个规则，删除其余冗余规则。
高风险放行规则	高风险威胁情报放行规则	高	检测到放行规则源IP、目的IP或域名命中威胁情报。	建议修改规则内容，避免遭受外部攻击。
	FTP高风险端口放行规则	高	检测到放行规则的目的端口为20/21端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
	DNS高风险端口放行规则	高	检测到放行规则的目的端口为53端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。

Elasticsearch高风险端口放行规则	高	检测到放行规则的目的端口为9200/9300端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
Hadoop高风险端口放行规则	高	检测到放行规则的目的端口为50070/8088端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
Kafka高风险端口放行规则	高	检测到放行规则的目的端口为9092端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
Memcached高风险端口放行规则	高	检测到放行规则的目的端口为11211端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
MongoDB高风险端口放行规则	高	检测到放行规则的目的端口为27017/27018端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
MySQL高风险端口放行规则	高	检测到放行规则的目的端口为3306端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
PostgreSQL高风险端口放行规则	高	检测到放行规则的目的端口为5432端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
RDP高风险端口放行规则	高	检测到放行规则的目的端口为3389端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
Redis高风险端口放行规则	高	检测到放行规则的目的端口为6379端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
SMTP高风险端口放行规则	高	检测到放行规则的目的端口为25端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
SSH高风险端口放行规则	高	检测到放行规则的目的端口为22端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
Telnet高风险端口放行规则	高	检测到放行规则的目的端口为23端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。

	VNC高风险端口放行规则	高	检测到放行规则的目的端口为5900-5902端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
	Zookeeper高风险端口放行规则	高	检测到放行规则的目的端口为2181/3888端口，属于高危端口。	建议调整端口范围，避免因端口暴露引发数据泄露或外部攻击风险。
无效规则	失效规则	高	检测到规则关联的资产实例、地址模板、或资源标签等模板已被部分删除。	建议直接删除该无效规则。
	被高优覆盖规则	低	检测到规则已被优先级更高的规则覆盖。	建议删除被覆盖的无效规则。
	源目相同规则	低	检测到规则的源IP与目的IP完全一致。	建议直接删除该无效规则。

日志管理

最近更新时间：2026-03-18 15:37:52

功能简介

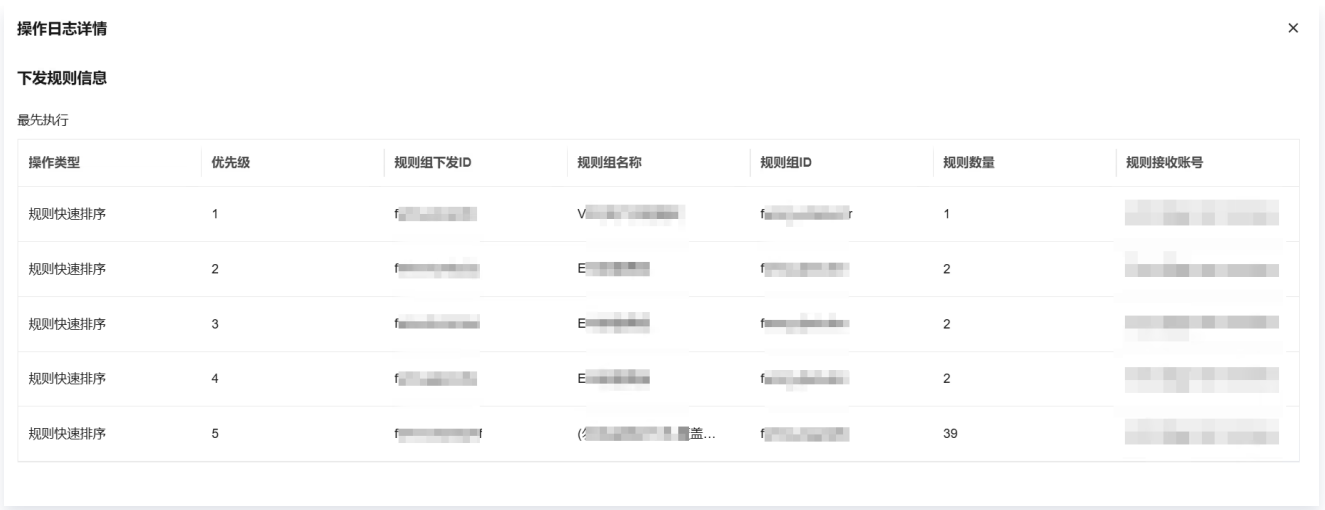
防火墙管理控制台提供日志管理功能，用于审计与追溯您的关键操作。该功能覆盖“策略管理”与“策略分析”两个模块，支持按时间范围筛选，并可组合多种资源属性进行精细化查询，帮助您快速定位目标日志并查看详情。

策略管理

1. 登录 防火墙管理控制台 ，在左侧导航中，选择**日志管理**。
2. 单击**操作日志 > 策略管理**。系统将默认展示近期的操作记录列表。
3. 在策略管理页面，您可以查看操作时间、操作账号、操作模块、操作行为等信息。
4. 您可以通过选择时间范围，并组合选择多种资源属性（如操作账号、操作行为等）进行精确查询，以快速过滤出目标记录。

5. 单击目标记录操作列的**详情**，即可查看该条操作日志的详细信息。
   - 查看**规则管理**模块的日志详情时，可查看对应规则组的基础信息及对应的规则信息。

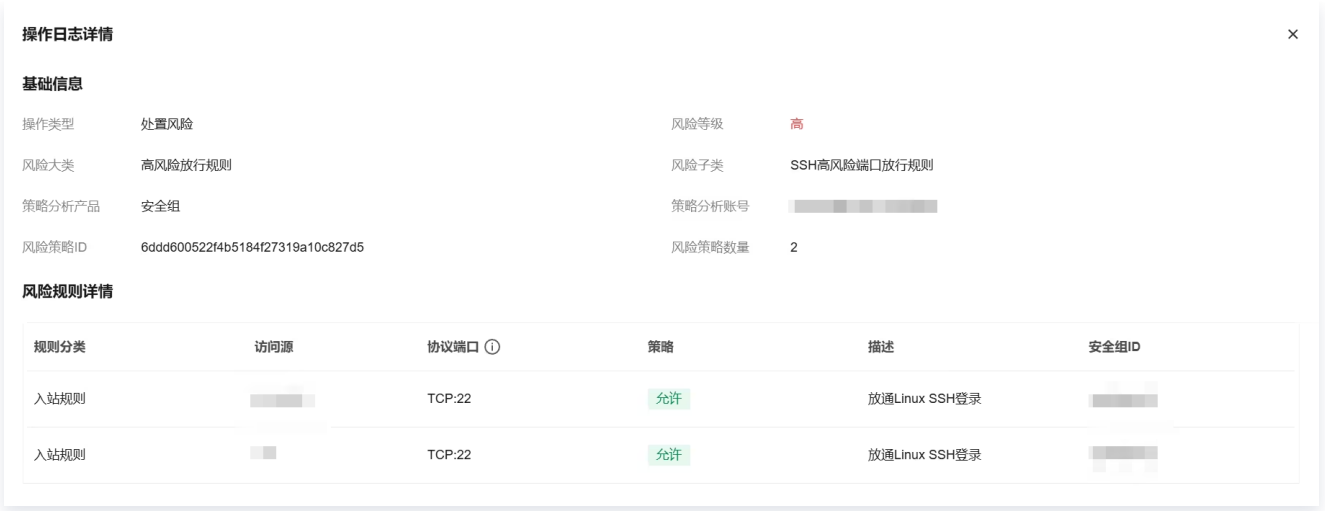
   - 查看**规则下发管理**模块的日志详情时，可查看相关下发规则的具体信息。



策略分析

1. 登录 防火墙管理控制台 ，在左侧导航中，选择**日志管理**。
2. 单击**操作日志** > **策略分析**。系统将默认展示近期的操作记录列表。
3. 在策略分析页面，您可以查看操作时间、操作账号、操作行为、体检产品等信息。
4. 您可以通过选择时间范围，并组合选择多种资源属性（如操作账号、操作行为等）进行精确查询，以快速过滤出目标记录。

5. 单击目标记录操作列的**详情**，即可查看该条操作日志的详细信息。
   - 查看**忽略风险**、**处置风险**以及**取消忽略**行为的日志详情时，可查看对应风险的基础信息及对应的风险规则信息。


操作日志详情

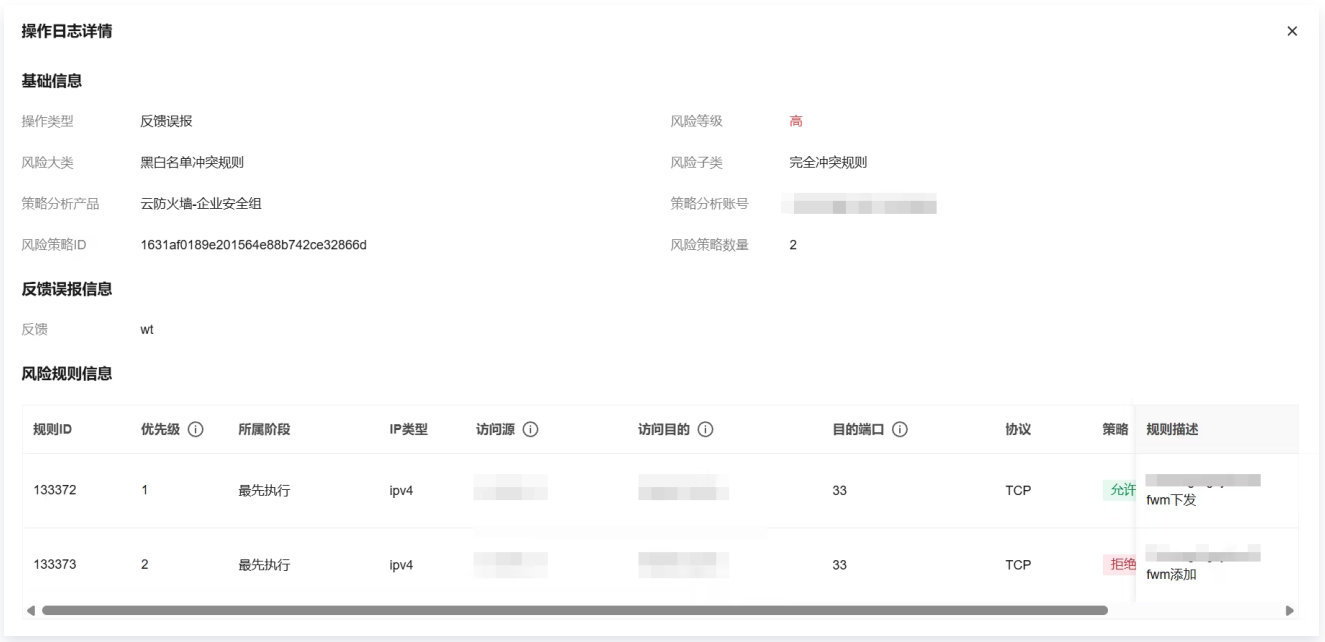
基础信息

操作类型	处置风险	风险等级	高
风险大类	高风险放行规则	风险子类	SSH高风险端口放行规则
策略分析产品	安全组	策略分析账号	
风险策略ID	6ddd600522f4b5184f27319a10c827d5	风险策略数量	2

风险规则详情

规则分类	访问源	协议端口	策略	描述	安全组ID
入站规则		TCP:22	允许	放通Linux SSH登录	
入站规则		TCP:22	允许	放通Linux SSH登录	

- 查看**反馈误报**行为的日志详情时，可查看对应风险的基础信息、反馈误报信息以及对应的风险规则信息。


操作日志详情

基础信息

操作类型	反馈误报	风险等级	高
风险大类	黑白名单冲突规则	风险子类	完全冲突规则
策略分析产品	云防火墙-企业安全组	策略分析账号	
风险策略ID	1631af0189e201564e88b742ce32866d	风险策略数量	2

反馈误报信息

反馈	wt

风险规则信息

规则ID	优先级	所属阶段	IP类型	访问源	访问目的	目的端口	协议	策略	规则描述
133372	1	最先执行	ipv4			33	TCP	允许	fwm下发
133373	2	最先执行	ipv4			33	TCP	拒绝	fwm添加

- 查看**开始体检**行为的日志详情时，可查看进行体检的产品信息、账号信息以及体检策略数量。


操作日志详情

体检产品	体检账号	体检策略数量
云防火墙-企业安全组		7