云防火墙

操作指南

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【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
防火墙开关
互联网边界防火墙开关
NAT 边界防火墙开关
VPC 边界防火墙
DNS 防火墙开关
自定义路由配置指引
防火墙引擎升级
防火墙引擎地域迁移
VPC 边界防火墙开关（主备模式）
概述
新建 VPC 边界防火墙（主备模式）
查看 VPC 边界防火墙（主备模式）
管理 VPC 边界防火墙（主备模式）
管理 VPC 边界防火墙实例（主备模式）
管理防火墙开关（主备模式）
使用网络拓扑（主备模式）
自定义路由配置指引（主备模式）
概述
私有网络模式
云联网模式
资产中心
概述
资产总览
资产列表
服务梳理
告警中心
概述
反馈误报
攻击告警事件查看与处理
告警事件查看与处理
拦截事件查看与处理
欺骗事件查看与处理
流量中心
访问控制
规则列表配额说明
互联网边界规则
NAT 边界规则
内网间规则
企业安全组
功能简介
配置步骤
实例间单向访问的自动双向下发
企业安全组(新)
配置步骤
企业安全组流日志
迁移指南
热点问题
特殊应用场景
访问控制概述
入侵防御

版权所有：腾讯云计算（北京）有限责任公司

开启威胁情报
开启基础防御
开启虚拟补丁
使用安全基线
管理防御操作
全流量检测与响应
零信任运维
概述
实践教程
通过 iOA 进行有端运维
通过微信或 iOA 进行无端运维
接入管理
概述
实例管理
资产接入
身份接入
域名接入
资产管理
概述
服务器管理
Web 服务管理
数据库管理
权限管理
概述
身份视角
规则视角
登录方式
微信用户公网远程登录服务器
iOA 用户内网访问运维资产
微信或 iOA 用户公网访问 Web 服务
网络蜜罐
概述
新建探针
管理探针
新建蜜罐服务
管理蜜罐
防御溯源
日志审计
日志分析
日志投递
日志字段
日志细类字段
访问控制类型
零信任防护日志
入侵防御日志
流量日志
操作日志
通知及设置相关
常用工具
地址模板
规则备份
自动化助手
网络抓包工具

版权所有：腾讯云计算（北京）有限责任公司

策略备份与回滚

操作指南
防火墙开关

版权所有：腾讯云计算（北京）有限责任公司

互联网边界防火墙开关

最近更新时间：2025-06-05 10:08:32

云防火墙提供互联网边界开关功能，在互联网边界开关页面，可自动探测到您所持有的公网 IP 以及关联的云上资产，并为您配置对应的防火墙开关。云防火墙开关支持一键开启防护，您无需进行任何的网络接入部署与路由策略配置，且无需安装任何镜像文件，云防火墙可以为您提供即开即用的产品体验。

接入模式说明

当前互联网边界防火墙支持串行和旁路两种部署模式，您可以自行选择不同的模式开启防护。
串行防火墙（Inline Firewall）和旁路防火墙（Bypass Firewall）是两种不同的防火墙部署方式，它们在网络中的位置和工作原理有所不同。

工作原理/部署类型	串行防火墙	旁路防火墙
部署路径	串行防火墙是直接部署在网络数据流的路径上，所有经过的数据包都需要经过防火墙的检查和处理。	旁路防火墙不是直接部署在网络数据流的路径上，而是通过镜像或端口复制等技术，获取网络流量的副本进行分析和检测。
处理数据	由于串行防火墙需要处理所有经过的数据包，因此对性能和处理能力有较高要求。 如果防火墙性能不足，可能会成为网络瓶颈，影响网络速度和稳定性。因此串行防火墙需要每个地域新建一个防火墙实例并分配对应带宽。	旁路防火墙只需要处理镜像流量，对性能和处理能力的要求相对较低。它可以在不影响网络性能的前提下，提供安全监控、拦截和告警功能。
安全防护	串行防火墙可以对数据包进行深度检查和处理，提供较高的安全保障。它可以阻止恶意数据包进入网络，保护内部资源免受攻击。	旁路防火墙的安全防护能力相对有限，仅能防护 TCP、HTTP/HTTPS和TLS/SSL 协议的流量，且腾讯云内部公网互访流量由于网络架构特性无法受旁路防火墙防护。旁路的架构可以通过抢答机制等技术，基于发送 TCP 的 RST 报文间接阻断攻击者与目标系统的连接。

说明：

- 串行模式支持地域：中国大陆地域、中国香港、新加坡、东京、首尔。
- 旁路模式支持地域：中国大陆地域。

支持资产类型

互联网边界防火墙支持如下资产类型：

产品名称		互联网边界防火墙（串行模式）	互联网边界防火墙（旁路模式）
云服务器 CVM		支持	支持
轻量应用服务器		不支持	支持
弹性公网 IP	常规 BGP IP	EIP 绑定实例后支持，详情以控制台是否可开启防火墙开关为准。如有疑问可提交工单 联系我们。	支持
	精品 BGP IP		支持
	加速 IP		支持
	静态单线 IP		支持
	高防 EIP		支持
	互联网通道（专线）	支持	支持
负载均衡 CLB	负载均衡 CLB	不支持	支持
	域名化负载均衡 CLB	不支持	支持
	IPv6负载均衡	不支持	不支持
	传统型负载均衡	不支持	支持

VPN 连接	不支持	支持
API 网关	不支持	支持
堡垒机	不支持	不支持

串行防火墙准备工作

在使用串行防火墙前，请先进行以下准备工作：

为串行防火墙分配带宽

由于串行防火墙具有地域集群属性，且存在防护性能上限，故需要用户为需要使用串行防火墙的地域分配带宽。

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关**页面，单击**防火墙设置**。

2. 为需要使用的串行防火墙地域分配带宽。建议根据业务峰值合理预估，**带宽超量后超过带宽的流量将不再防护**，该过程不会影响网络，具体可参考 互联网边界防火墙带宽超量处置 。

> **说明：**
> - **通用带宽：当前版本为串行防火墙分配带宽将消耗通用带宽，通用带宽与 NAT 边界防火墙共享。**
> - **通用实例：当前版本每新增1个串行防火墙地域将消耗1个通用实例配额，通用实例配额与 NAT 边界防火墙共享。**

- 串行防火墙地域：当前版本支持的地域以串行防火墙设置展示地域为准，更多地域正在逐渐灰度中，敬请期待。

确认资产符合防护范围

- 由于网络架构限制，当前版本串行防火墙仅支持防护最新网络架构的弹性公网 IP，具体以控制台显示为准，如有疑问可与弹性公网 IP 团队联系确认。暂不支持防护公网 CLB 类型，如需防护建议切换为 EIP + 内网 CLB 的形式可支持防护。
- 当前版本旁路防火墙支持的资产类型为：云服务 CVM、NAT 网关、VPN 网关，轻量级服务器 LH，负载均衡 CLB 等。

串行防火墙开关操作

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关 > 防护对象 > 互联网边界**。
2. 在互联网边界页面，找到需要防护的资产，请确认接入模式显示为**串行**。

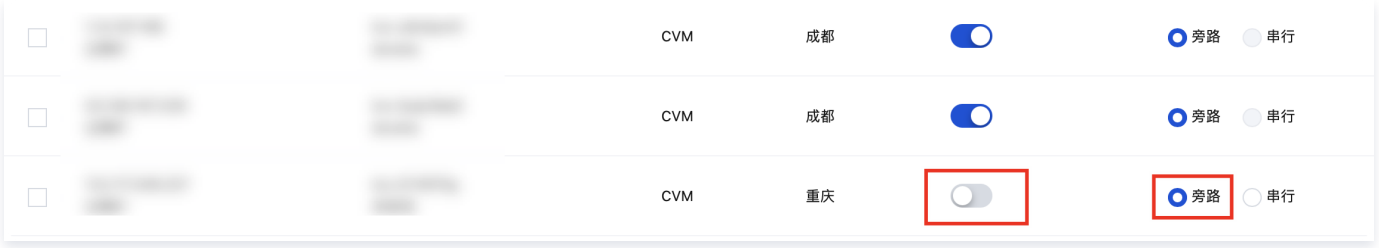
3. 单击防火墙开关列的，即可对该资产进行边界防护。
4. 开启串行防火墙过程预计耗时 1 分钟，对网络无影响。

说明：

- 串行模式需要使用 私有连接 打通 VPC 到防火墙的网络。
- 同一个 VPC 内的 EIP 首次启用串行防火墙时，需要创建新的私有连接的 终端节点 与引流内网 IP，您在串行防火墙规格（分配的带宽）内的私有连接无需额外付费，超量可能会产生一定费用，详情请参见 私有连接收费标准 。后续相同 VPC 内串行防火墙开关无需再次创建私有连接。

旁路防火墙开关操作

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关 > 防护对象 > 互联网边界**。
2. 在互联网边界页面，找到需要防护的资产，请确认接入模式显示为**旁路**。



3. 单击防火墙开关列的，即可对该资产进行边界防护。

说明：

- 当前版本支持的资产类型为：云服务 CVM、负载均衡 CLB、NAT 网关、VPN 网关，轻量级服务器 LH，目前支持中国大陆及中国香港地域资产。
- 开启开关：当开启开关时，该公网 IP 的所有流量将经过云防火墙，且访问控制、入侵防御、日志审计功能将对该公网 IP 生效。
- 关闭开关：当关闭开关时，该公网 IP 的所有流量将不会经过云防火墙。

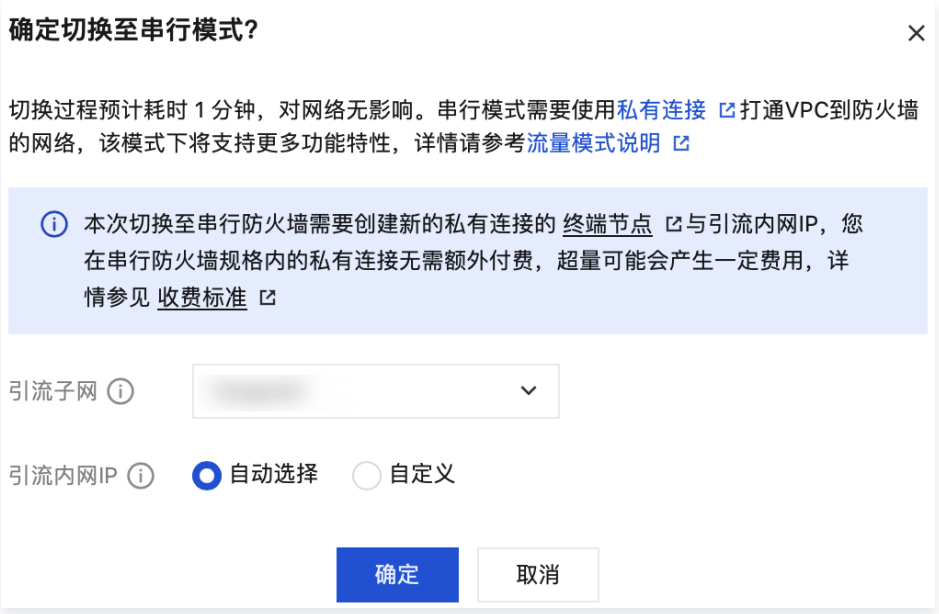
切换接入模式

登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **防护对象** > **互联网边界**。

切换单个开关流量模式

1. 在互联网边界页面，当防火墙开关状态为**关闭**的情况下，选择想要切换的接入模式即可，对网络无影响。

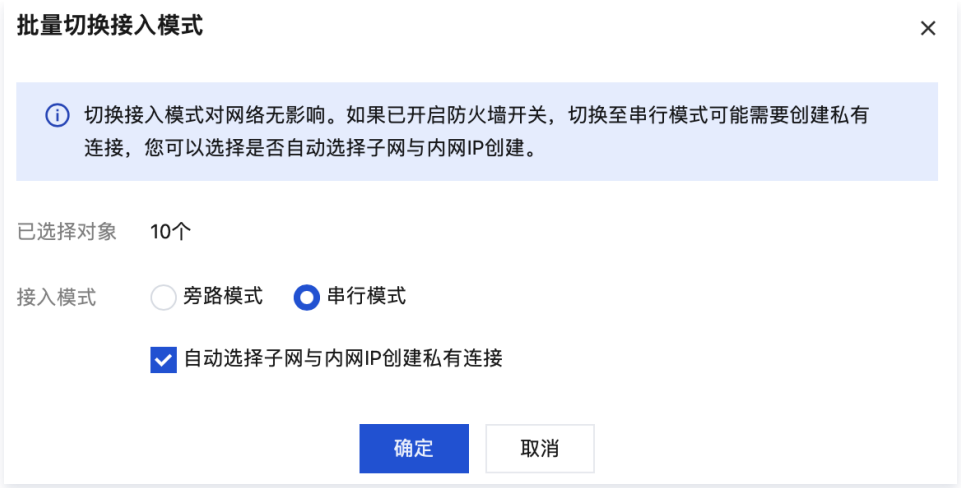
2. 如果防火墙开关为**开启**状态，切换接入模式会触发串行防火墙开关的开启或关闭操作，详情请参见 串行防火墙开关操作 。



批量切换防火墙开关接入模式

1. 在互联网边界页面，勾选需要进行切换的防火墙开关，单击**切换模式**。

2. 确认需要切换接入模式，单击**确定**。如果是串行模式，可选择是否需要自动选择子网与内网 IP 创建私有连接。



防火墙状态监控

用户可以实时查看并监控基于公网 IP 的带宽情况，从而及时作出扩容或关闭部分开关等调整。

1. **在状态监控面板右上角，单击 图标。**

2. **在状态监控页面，可实时查看并监控基于公网 IP 的带宽情况，并进行扩容或关闭部分开关等操作。**

> **说明：**
> **峰值带宽指上行和下行的最大值，即如果购买100M带宽，那么云防火墙能够同时处理上行100M和下行100M。**

新资产自动开启

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关**页面，单击**防火墙设置**。

2. 单击**功能配置** > **新资产自动开启开关**，可在防护公网 IP 配额允许的情况下，对于新增的公网 IP 资产，将自动开启互联网边界开关。您可以在下方选择是否选择默认开启串行接入模式和是否自动创建私有连接。

互联网边界防火墙超量 Bypass 权重设置

- 您可以通过自定义开关权重，流量超过互联网边界防火墙规格后，我们会按照您定义的开关权重等级依次 Bypass 直至当前地域带宽降至规格内。
- 相同权重会自动按照峰值带宽降序依次关闭。初始权重默认为1，最大为100，最小为0，权重越大优先级越高。

操作步骤

1. 登录 **云防火墙控制台**，在左侧导航栏中，选择**防火墙开关**页面，单击**防火墙设置**。

2. 在**防火墙设置 > 功能配置**页面，编辑指定防火墙开关权重。

3. 单击**编辑权重**，可以选择防火墙开关，批量编辑开关权重，单击**确定**保存。

同步资产

- 后台定时轮询用户资产信息的间隔为5分钟，因此当用户资产规模在此间隔内发生变化，但尚未被后台同步时，可在列表上方，单击**同步资产**，及时调用后台接口重新读取并同步用户的资产信息与数据。
- 当新增的资产没有出现在防火墙开关列表时，您可以在列表上方，单击**同步资产**进行同步资产尝试。

查看规则、告警或日志

除了在资产列表开启防火墙开关，可以执行一些其它操作，主要包括查看资产关联的规则、告警和日志。

- 查看规则：在资产列表中，单击操作列的**查看规则**，将跳转到资产所关联的规则页面。

- 查看告警：在资产列表中，单击操作列的**更多 > 查看告警**，选择具体的事件类型，将跳转到告警中心相应的事件页面。

- 查看日志：在资产列表中，单击操作列的**更多 > 查看日志**，选择具体的日志类型，将跳转到相应的日志页面。

互联网边界防火墙带宽超量处置

互联网边界防火墙的带宽超负荷不会导致客户业务流量丢包或影响流量速率，但将无法提供防护功能。

自2024年09月25日起，业务带宽超过互联网边界防火墙带宽100%时，将采取以下措施：

- 关闭部分互联网边界防火墙开关，将一部分流量 Bypass 转发，只防护带宽规格的流量。
- 串行和旁路模式处置方法一致，关闭部分开关限制流量。
- 支持配置防火墙开关权重，设置自动关闭防火墙开关的优先级。

更多详情请参见 常见问题–带宽相关 。

相关信息

- 如需对内网资产进行流量管控与安全防护，或基于 SNAT、DNAT 进行的网络流量转发，可参见 NAT 边界防火墙开关 进行操作。
- 如需自动探测 VPC 信息与互通关系，并在每一对互通的 VPC 间，建立云防火墙开关，可参见 VPC 间防火墙开关 进行操作。
- 如遇到互联网边界防火墙相关问题，可参见 防火墙相关 文档。

NAT 边界防火墙开关

最近更新时间：2025-06-18 09:47:32

0NAT 边界防火墙开关支持基于内网资产进行流量管控与安全防护，同时支持基于 SNAT、DNAT 进行的网络流量转发。

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **NAT 边界开关**。

> **说明：**
> 当某个 NAT 边界防火墙开关开启后，对应子网的互联网流量将经过防火墙，届时访问控制规则、入侵防御功能将对其生效，流量日志也会生成。

2. 在 NAT 边界开关页面，可进行创建实例、同步资产、查看并监控基于 NAT 边界的带宽情况等操作。

创建实例

1. 在 NAT 边界开关页面 下，单击**创建实例**。

2. 在新建 NAT 边界防火墙弹窗中，可为当前账号创建一个新的 NAT 边界防火墙实例，填写相关字段，单击**下一步**。

> **说明：**
> 创建“NAT 边界防火墙”实例，涉及大量后台配置工作，这个步骤可能需要持续若干分钟。

字段说明：

- **地域**：选择创建地域，支持中国大陆、中国香港、中国台北与部分海外地域，创建实例后不可更改。

  > **说明：**
  > 用户可在拥有 VPC 的中国大陆、中国香港、中国台北与部分海外地域中进行地域选择，同地域下可创建多个防火墙实例，但总带宽不能超过限定规格。

- **可选区**：根据需求选择合适的可用区。
- **实例名称**：输入实例名称。
- **实例规格**：根据需求选择实例规格，最小20Mbps，如需更多带宽请 升级扩容 。实例规格和规则数规格匹配，详情请参见 实例规格 。

  > **说明：**
  > 互联网带宽保持一致，如果分了多个 NAT 防火墙，那么多个 NAT 防火墙的带宽之和，要小于等于互联网边界的带宽。

- **模式**：分为新增模式和接入模式。
  - **新增模式**：若当前地域没有 NAT 网关，新增模式可以通过 NAT 边界防火墙内置的 NAT 功能，实现指定实例通过防火墙访问互联网。
  - **接入模式**：若当前地域已有 NAT 网关，或者希望公网对外的出口 IP 保持不变，接入模式可以将 NAT 边界防火墙平滑接入到 NAT 网关与 CVM 实例之间。
- **弹性 IP**：新增模式下云防火墙支持选择闲置未使用的弹性公网 IP 进行绑定，同时支持快速创建弹性公网 IP；若选择新建弹性 IP，系统会自动通过CAM为用户申请一个弹性 IP。

  > **说明：**
  > 请注意弹性公网 IP 的带宽需要大于等于防火墙的防护带宽，否则将出现防护带宽过剩的情况。弹性公网 IP 的费用由 EIP 产品收取，防火墙不收取任何 EIP 带宽费用。

3. 选择需要接入的 VPC 或 NAT 后，进行防火墙网络配置，选择**新建引流子网方式**。建立引流子网的方式包括以下三种：

说明：
- 引流子网：云防火墙会在您所接入的 VPC 中新建24网段的子网，用于将流量牵引至防火墙，您可以选择不同的创建子网的方式。
- 600M以下NAT防火墙实例：新增模式最多支持8个 VPC，接入模式最多支持4个 NAT 网关。
- 600M以上NAT防火墙实例： 新增模式最多支持10个 VPC，接入模式 最多支持5个 NAT 网关。

- 自有网段优先：云防火墙会在所选的 VPC 内自动选择空闲子网网段；当 VPC 内无子网配额时，会使用所选 VPC 的扩展网段。
- 扩展网段优先：云防火墙会优先使用空闲的 VPC 保留的扩展网段，该模式下不会占用所选 VPC 子网配额。

说明：
扩展网段是指私有网络中的辅助网段，可参见 私有网络–编辑 IPv4 CIDR 。

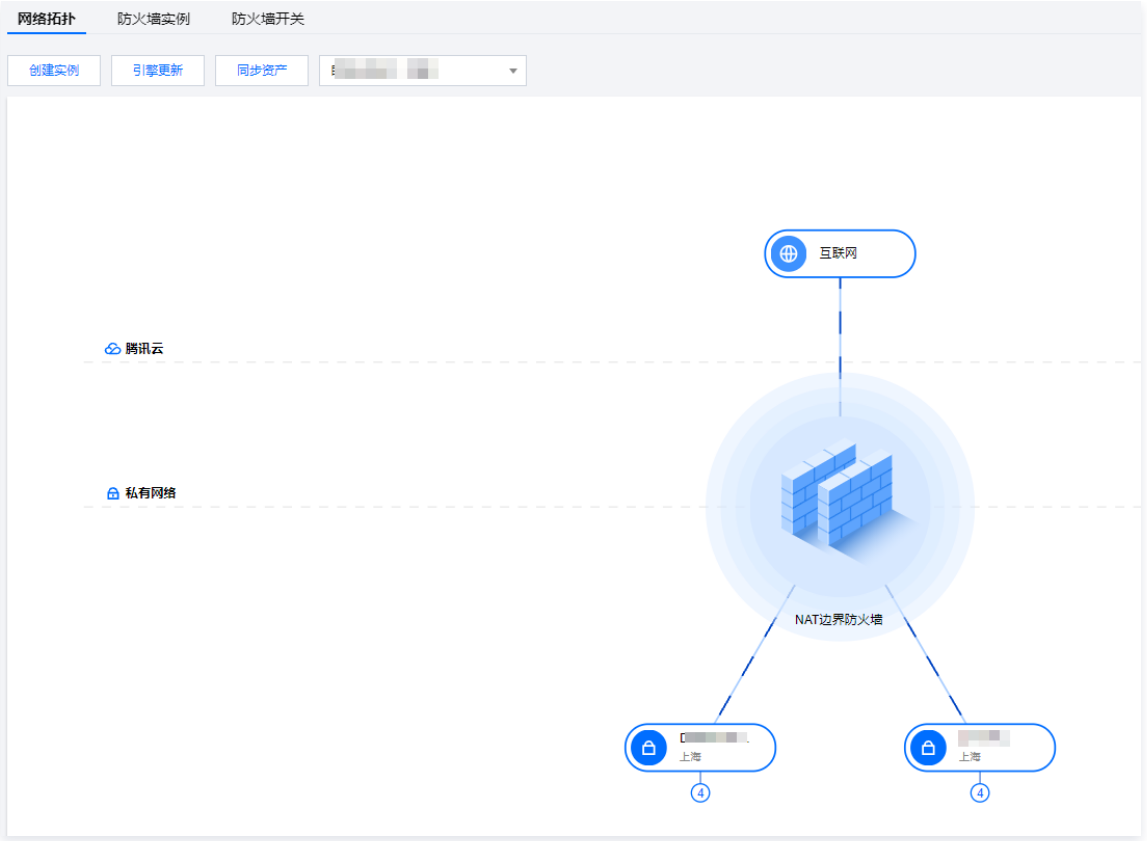
- 自定义：用户可以自定义供防火墙使用的子网网段，请注意必须为24网段；自定义网段必须属于当前 VPC 的 CIDR。输入示例：192.168.0.0/24。

4. 配置完成后，单击**创建**，即可成功创建 NAT 边界防火墙。

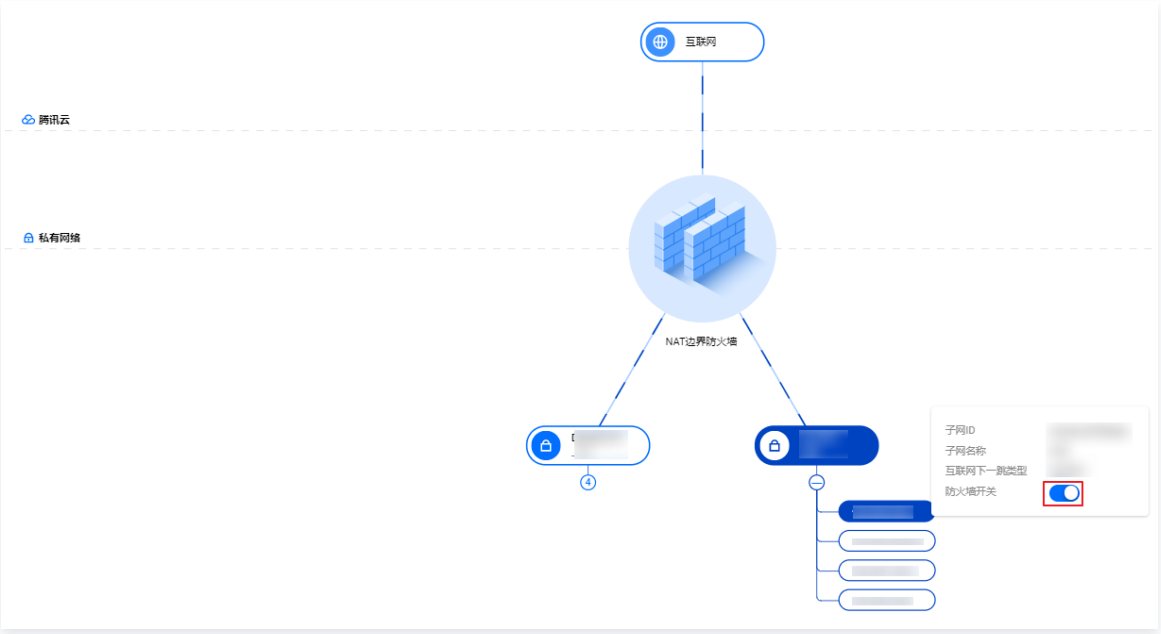
网络拓扑

云防火墙提供了一个可视化视图，帮助您快速梳理 NAT 边界的访问关系。在 NAT 边界可视化视图中，私有网络展现了 VPC 实例。

1. 在 NAT 边界开关页面 下，单击**网络拓扑**，可查看 NAT 边界的访问关系。



2. 单击某个 VPC 节点，可查看对应子网列表，可以只针对当前子网开启或关闭防火墙开关。



防火墙开关

在 防火墙开关页面，支持开启或关闭 NAT 边界防护。云防火墙会定时自动同步云资产，因此不用担心资产变更后的防火墙配置（例如，变更了某个子网，防火墙会在短时间内自动同步）。

- **开启防护**
  - 在实例列表上方，单击**全部开启**，所有未开启的 NAT 边界防火墙开关将被打开，所有路由表将会自动添加下一跳类型为 NAT 边界防火墙的路由策略，所有子网的互联网流量将会经过 NAT 边界防火墙。

> **注意：**
> - 开启开关后，请勿在 私有网络控制台 中手动变更开关对应的路由，否则将导致防火墙丢失路由而引发网络中断。

- 若用户选择开启同一路由表关联的所有子网，系统会自动在该路由表中增加一条下一跳指向 NAT 边界防火墙的路由策略，并关闭原访问公网的路由策略，因此该路由表关联的所有子网的互联网流量，将会经过 NAT 边界防火墙。
- 如果防火墙实例为接入模式，请确保对应 NAT 网关 SNAT 规则图示处开关为关闭状态，否则防火墙引流策略将不会生效。

- 一个防火墙开关对应一个子网，用来控制流量是否经过 NAT 边界防火墙，关联了同一个路由表的子网将会同时开启或关闭，创建 NAT 边界防火墙后，防火墙不会立即引流，需要您前往防火墙开关页面手动开启。

> **说明：**
> 开启开关后，系统会自动修改子网关联路由表的路由策略，以及子网对应的端口转发规则，该子网的流量牵引至 NAT 边界防火墙。

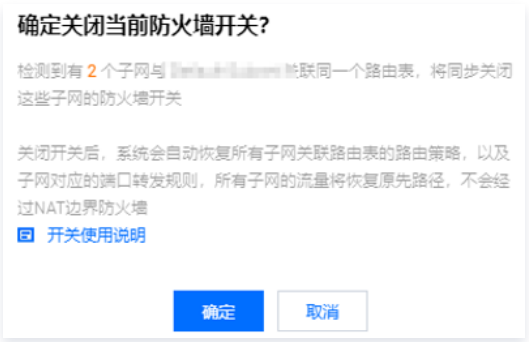
- **关闭防护**
  - **方式1**：在实例列表上方，单击**关闭防护**，所有已开启的 NAT 边界防火墙开关将被关闭，NAT 边界防火墙会自动关闭下一跳类型为 NAT 边界防火墙的所有路由表的路由策略，所有子网将断开与互联网的连接，用户需要在 私有网络控制台 手动启动新的路由策略。

> **说明：**
> 若用户选择关闭同一路由表关联的所有子网，系统会自动关闭该路由表中下一跳指向 NAT 边界防火墙的路由策略，该路由表关联的所有子网将会断开与互联网的连接。

  - **方式2**：单独关闭防火墙开关。
    如想单独关闭防火墙开关，可以在防火墙开关操作栏，单击某个子网的“防火墙开关”按钮，其它关联了同一个路由表的子网也将会同时关闭。

> **说明：**

关闭开关后，系统会自动恢复子网关联路由表的路由策略，以及子网对应的端口转发规则，该子网的流量将恢复原先路径，不会经过 NAT 边界防火墙。

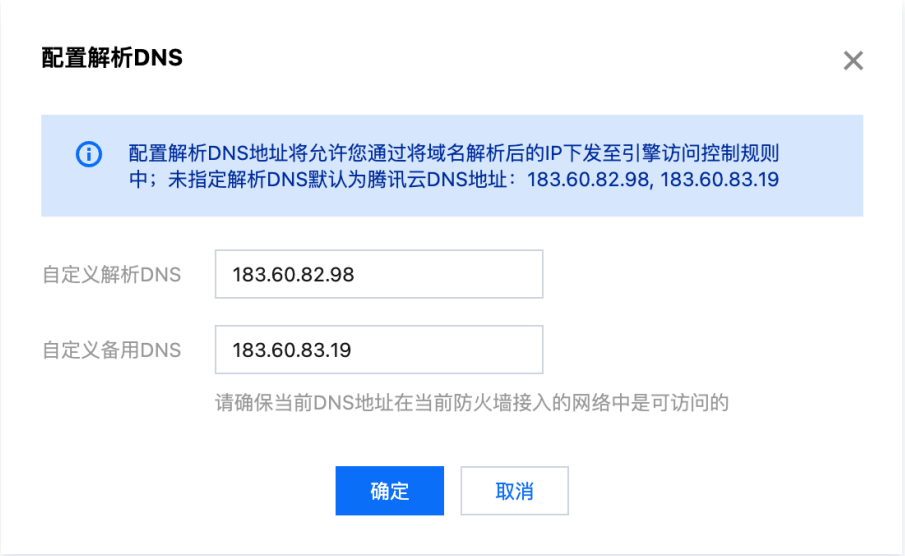


网络配置

1. 在 NAT 边界开关 > **防火墙实例**页面，选择所需实例，单击**更多** > **网络配置**。

2. 单击**配置解析DNS**，可以配置用于域名解析类型的访问控制规则的自定义DNS解析服务器地址。
3. 在配置解析 DNS 窗口中，填写相关参数，单击**确定**保存。

说明：
默认情况下，将使用腾讯云默认的 DNS 服务器地址，分别为183.60.82.98和183.60.83.19。如果您需要指定 DNS 服务器进行解析，请在下方填写。



实例配置

在 NAT 边界开关页面 下，单击对应**实例 ID**，或者单击防火墙实例右侧的**实例配置**，可以进入实例配置的界面。

- **端口转发**
  在右侧边栏中可以查看用户基于 NAT 边界防火墙实例所添加的 DNAT 端口转发规则，以及与实例关联的弹性 IP。

> **说明：**
> - 接入模式中，首次开启开关后，NAT 边界防火墙会自动同步现有NAT网关的端口转发规则，从而保证流量通行，后续对于该规则的操作，请在 云防火墙控制台 中进行。
> - 开启防火墙开关的子网 SNAT、DNAT 流量都会经过防火墙，关闭开关的子网 SNAT、DNAT 流量都走原先路径。
> - 请勿前往私有网络控制台操作端口转发规则，否则可能造成网络中断。

1.1 在实例配置页面的端口转发页签下，单击**新建规则**。

1.2 在“新建端口转发规则”弹框中，用户可为当前 NAT 边界防火墙实例添加一条外部 IP 为用户所绑定的弹性 IP 的 DNAT 规则。

> **说明：**
> - 在外部 IP 端口下拉框内，提供的选项为当前 NAT 边界防火墙实例所绑定的弹性 IP。
> - 输入内部 IP 地址时，用户需填写本地域 VPC 网段内可用的 IP。

- **出口绑定**

  在新增模式下，当规则列表为空时，所有 VPC 的子网将随机选择 NAT 网关访问互联网。

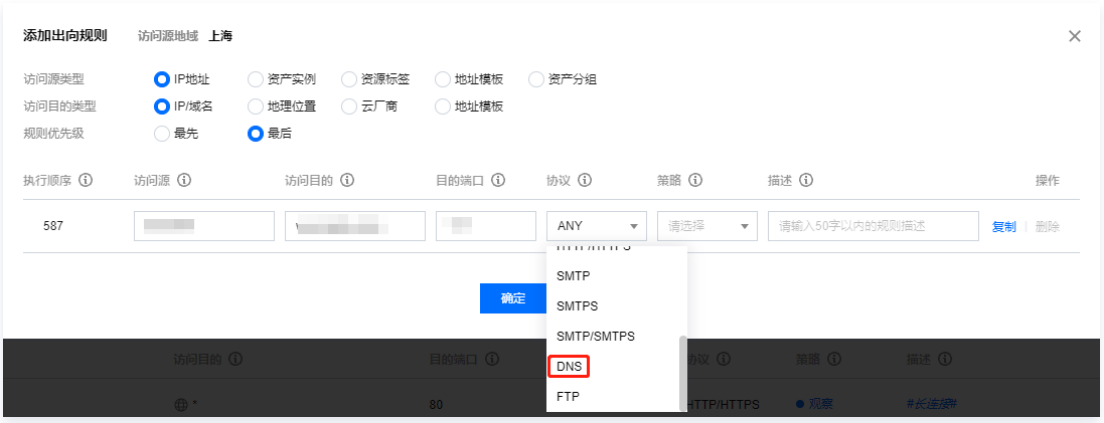
  > **注意：**
  > 接入模式暂不支持出口绑定。

  1.1 在实例配置页面的出口绑定页签下，单击**新建规则**。

  1.2 在“新建出口绑定规则”弹框中，提供防火墙实例 ID 信息，用户可为当前 NAT 边界防火墙添加 SNAT 规则。

  > **说明：**
  > - 实例类型可选私有网络、子网和云服务器。仅支持选择已接入 NAT 边界防火墙，且当前没有绑定出口 NAT 规则的实例。
  > - 独占 IP 选项可将所选的外部 IP 地址作为独占规则的子网/私有网络的出口 IP，而不能被独占规则外其他子网/私有网络使用。

- 接入 DNS 流量
  - 由于腾讯云底层架构，PrivateDNS（183.60.83.19,183.60.82.98）流量不会经过防火墙，所以无法受 NAT 边界防火墙防护。除 PrivateDNS 外的其他 DNS 流量可以经过防火墙。
  - PrivateDNS：请使用 DNS 防火墙防护，详情参考DNS防火墙开关。
  - 其他 DNS：防火墙默认支持防护此类流量，无需额外启用开关。
  - **应用场景**：对于其他 DNS，您可以在访问控制规则中添加 DNS 规则以限制访问。
    - 在 NAT 边界规则 页面，单击**出向规则**。
    - 在出向规则页签中，单击**添加规则**。
    - 在添加规则页面，填写相关字段，并选择 DNS 协议，单击**确定**。



- **关联弹性 IP**

1.1 在实例配置页面右侧的“关联弹性 IP”模块，单击**+绑定弹性 IP**。

1.2 在单选下拉框内，用户可为当前 NAT 边界防火墙实例绑定一个系统新建的弹性 IP，或在当前地域拥有的所有闲置弹性 IP 里选择一个进行绑定。

> **说明：**
> - 关联弹性 IP 功能目前只支持新增模式。
> - 解除绑定某个弹性 IP 时，页面上与其相应的 DNAT 规则也会消失。

- **带宽限速**

  在实例配置页面的带宽限速页签下，可以对当前防火墙实例下的 IP/CIDR 地址进行带宽限速。

  > **说明：**
  > NAT 网关限速机制在流量统计结束后触发，因统计与限速生效存在时间窗口，可能导致 NAT 网关上流量监控数据存在差异。

- **新增限速**

  1.1 单击**新增规则**，弹出添加限速规则弹窗。

  1.2 输入需要限速的 IP/CIDR 地址，以及限制的带宽速率，入向速率与出向速率中至少填入一个限制速率，不填写的默认无限制。单击**确定**，完成带宽限速设置。

  > **注意：**
  > 仅支持填写内网 IP。

- 编辑限速

  1.1 在已设置成功的限速规则中，单击操作栏中的**编辑**，进行规则编辑操作。

  1.2 重新输入需要限速的 IP/CIDR 地址，以及限制的带宽速率，入向速率与出向速率中至少填入一个限制速率，不填写的默认无限制。单击**确定**，完成带宽限速设置。

- 删除限速

  在已设置成功的限速规则中，单击操作栏中的**删除**，即可删除带宽限速规则限制。

规格调整

1. 在 NAT 边界开关 页面下，单击**升级扩容**，跳转到配置变更页面，在此页面可以升级带宽、版本、日志存储量等参数。

> **说明：**
> 这里升级扩容如果只扩容带宽，这个带宽指的是互联网边界带宽，也可以理解为云防火墙的总带宽。

2. 如果要对单个 NAT 边界防火墙实例带宽扩容，可按如下步骤操作：

> **说明：**
> - 调整的范围与互联网带宽保持一致，如果分了多个 NAT 防火墙，那么多个 NAT 防火墙的带宽之和，要小于等于互联网边界的带宽。
> - 如果目标带宽超过当前购买的带宽规格，可以单击 **升级扩容**，来调整互联网边界带宽。
> - 如果是小范围调整带宽，无需切换网络。在较大范围调整带宽时（涉及到升级实例规格档位，详情请参见 **实例规格** ），后台需要重新配置网络，可能会有3-5s的网络闪断。

2.1 在 **NAT 边界开关** > 防火墙实例页面，找到需要调整带宽的实例，单击**实例 ID** 或者右侧的**实例配置**。

2.2 在防火墙实例页面，单击右上角的**规格调整**。

2.3 分配好带宽后，单击**确定**，等待后台调整完成。

实例规格

NAT 防火墙实例规格档位表。

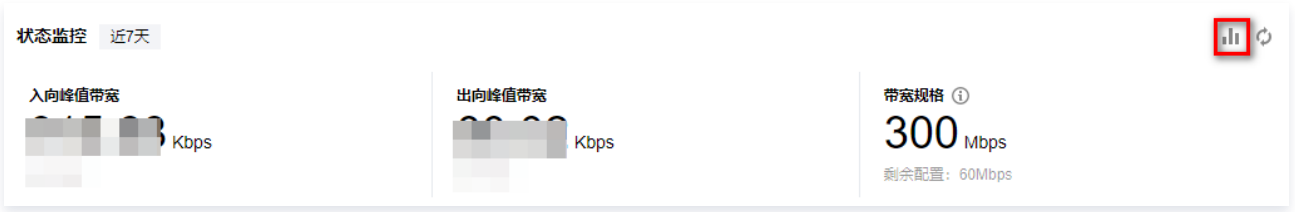
> **说明：**
> - NAT 实例规格与 NAT 规则列表配额互相独立，不涉及计费逻辑，无法额外单独扩容，仅能通过提升实例规格实现。您每在控制台配置一条 ACL，我们会自动按照下发公式帮您转换为特定规则，并自动识别访问源和访问目的，下发到指定 NAT 防火墙实例上。
> - 下发公式：下发规则数 = 源地址个数 × 目的地址个数 × 端口个数 × 协议个数。
> - NAT 实例规格决定了每个 NAT 防火墙能承载的最大 ACL 规则数量，当 ACL 下发数量过多时可能会导致引擎出现不稳定的情况。
> - 为了避免给您的业务造成影响，我们建议您根据每个实例的规格和下发规则数合理优化规则，减少冗余规则的占比，提升引擎稳定性。

规格档位	最低带宽/Mbps	最高带宽/Mbps	并发连接数/个	规则数配额/条
1	0	299	130,000	5,000
2	300	1,300	130,000	20,000
3	1,301	4,095	150,000	40,000
4	4,096	6,143	300,000	60,000
5	6,144	10,239	500,000	120,000
6	10,240	102,400	1,000,000	200,000

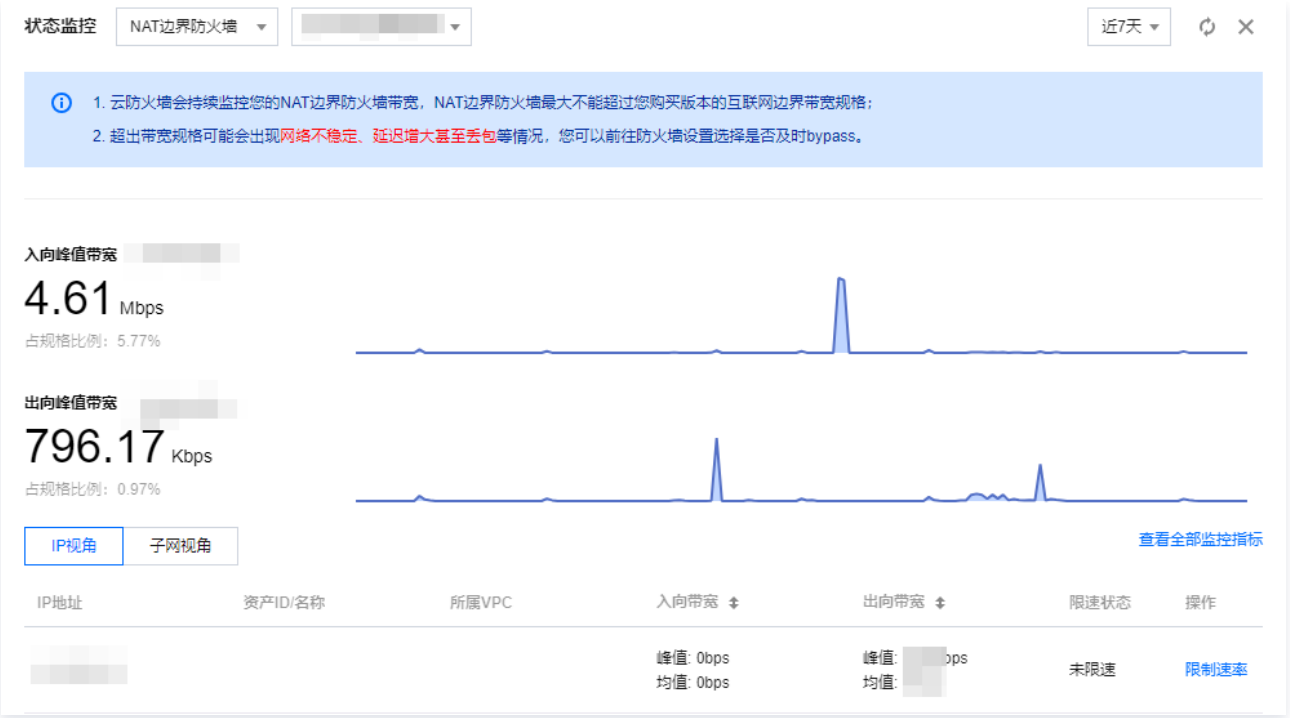
监控情况

在 NAT 边界开关 页面，可进行查看并监控基于 NAT 边界的带宽情况、同步资产、网络拓扑等。

1. 在状态监控面板右上角，单击，进入防火墙状态监控页面。



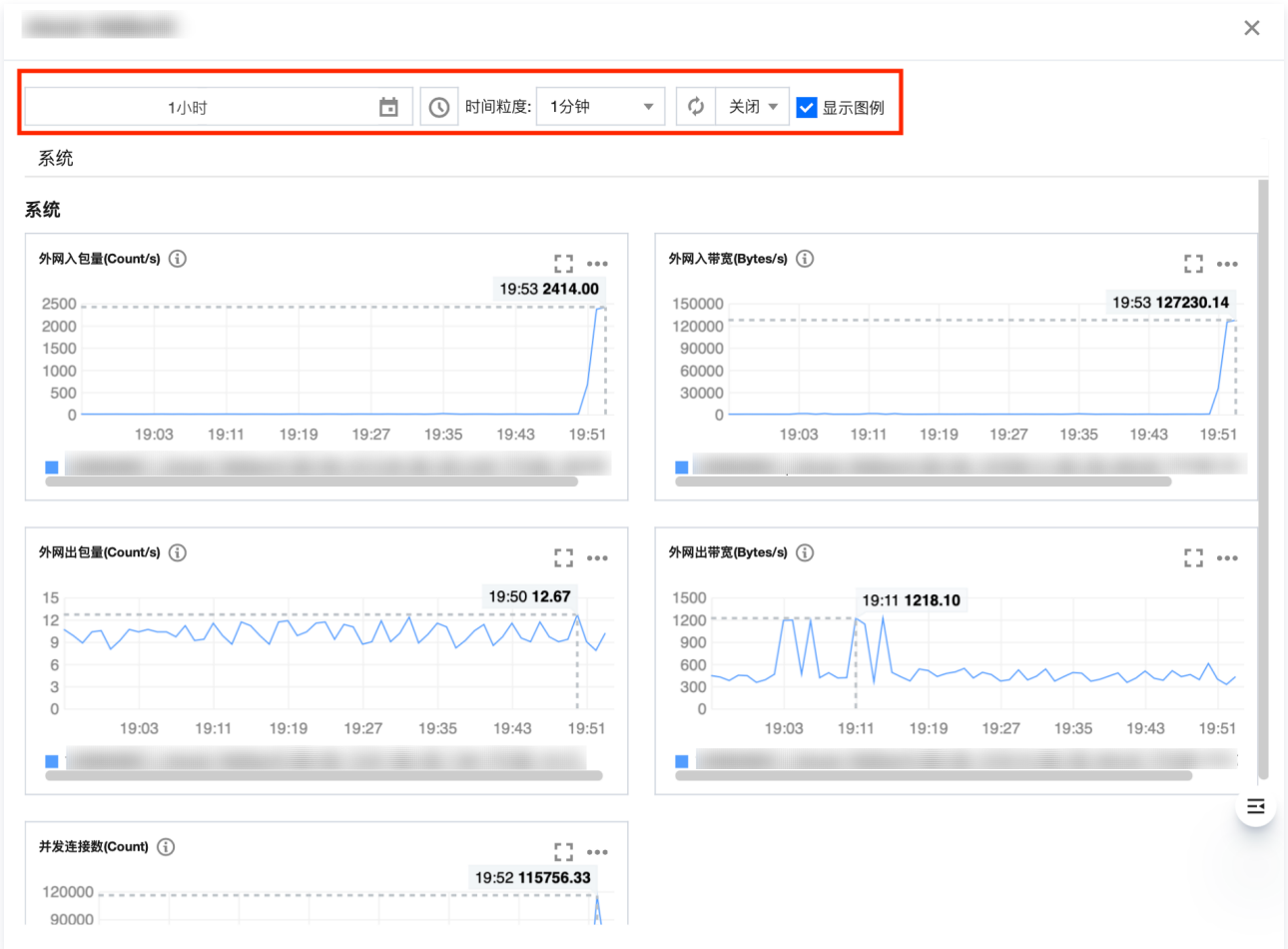
2. 在防火墙状态监控页面，可实时查看并监控基于 NAT 边界的带宽情况，可避免因 NAT 边界防火墙带宽超出规格而带来网络丢包和波动，从而及时作出扩容或关闭部分开关等调整。



3. 在防火墙状态监控页面，支持以 IP 视角与子网视角查看带宽状态监控。
   - IP 视角：IP 地址的资产信息、所属 VPC、入向/出向带宽的峰值与均值情况、限速状态、限制速率操作。
   - 子网视角：子网名称、IPv4 CIDR 地址、入向/出向峰值带宽、开关状态、查看开关操作。

4. 单击**查看全部监控指标**，可以查看该实例下更多监控指标数据，包括入/出包量数据等；您也可以前往 腾讯云可观测平台 查看更多数据内容。

5. 可设置监控数据的时间间隔、同比/环比、刷新时间等配置信息。



同步资产

在 NAT 边界开关 > 防火墙实例页面，单击**同步资产**，可以主动调用后台接口重新读取并同步用户子网的资产信息，可避免发生因用户资产规模在后台轮询间隔内发生变化，但尚未被同步的情况。

对 VPC 及 NAT 进行其他操作

增加接入 VPC/NAT

- **新增模式：**

1.1 在 NAT 边界开关 > 防火墙实例页面，单击**更多** > **接入配置**，在下拉框中，单击**增加接入 VPC**。

1.2 在增加需要接入的 VPC 弹框中，选择需要的 VPC，单击**确定**，即可配置完成。

> **说明：**
> - 支持私有网络 ID/名称、IPv4 CIDR 关键字搜索。
> - 复选框：默认已点选用户当前 VPC，已选择的 VPC 无法取消。
> - 单击**增加需要接入的 VPC**后，即触发当前地域下 NAT 边界防火墙开关锁，直至重新选择完毕，单击**确定**后解锁。在开关锁期间，若有当前地域其他用户有开启开关请求，会提示有其他用户正在重新接入 VPC，开关被锁定，请稍后重试。

- **接入模式：**

  1.1 在 NAT 边界开关 > 防火墙实例页面，单击**更多** > **接入配置**，在下拉框中，单击**增加接入 NAT**。

  1.2 在需要增加接入的 NAT 弹框中，选择需要接入的 NAT，单击**确定**，即可完成配置。

  > **说明：**
  > - 支持关键字模糊搜索：支持 NAT 实例 ID/名称、关联弹性 IP、私有网络 ID/名称搜索。
  > - 复选框：默认已点选用户当前NAT防火墙实例已经接入的 NAT 网关并无法取消。

重新选择接入 VPC/NAT

- **新增模式：**

  1.1 在 NAT 边界开关 > 防火墙实例页面，单击**更多** > **接入配置**，在下拉框中，单击**重新选择接入 VPC**。

  > **注意：**
  > 必须关闭当前防火墙实例下的所有子网开关和 DNS 流量开关。

  1.2 在选择需要接入的 VPC 中，可查看用户当前地域的 VPC，选择需要接入的 VPC，单击**确定**，即可配置完成。

  > **说明：**
  > - 支持关键字模糊搜索：支持私有网络 ID/名称、IPv4 CIDR 关键字搜索。
  > - 复选框：默认已点选用户当前VPC，已选择的VPC无法取消。

- **接入模式**

1.1 在 NAT 边界开关 > 防火墙实例页面，单击**更多 > 接入配置**在下拉框中，单击**重新选择接入 NAT**。

> **注意：**
> 请先检查开关是否全部关闭，重新选择接入 NAT 需要关闭全部开关（不包含关闭中的开关）。

1.2 在选择需要接入的 NAT 中，显示用户当前地域的NAT实例，选择需要接入的 NAT。

> **说明：**
> 单击**选择需要接入的 NAT**后，即触发当前地域下 NAT 边界防火墙开关锁，直至重新选择完毕，单击**确定**后解锁。在开关锁期间，若有当前地域其他用户有开启开关请求，会提示有其他用户正在重新接入 NAT，开关被锁定，请稍后重试。

销毁实例

1. 在 NAT 边界开关 > 防火墙实例页面，单击**更多**，在下拉框中，单击**销毁实例**。

> **注意：**
> - 销毁实例前必须关闭全部防火墙开关。
> - 用户由于业务变更，需要自主销毁实例，可自行在页面操作。
> - 销毁实例后会删除这个实例的所有配置，会保留日志，销毁完毕，会归还配额，自动恢复为原先的路由和端口转发，更新地域展示情况，只展示剩余地域。若无剩余地域，则页面回到创建实例初始页。

2. 在弹出的确认框中，单击**确定**，即可删除这个实例的所有配置。

调试工具

在 NAT 边界开关 > **防火墙实例**页面，单击**更多**，在下拉框中，单击**调试工具**。

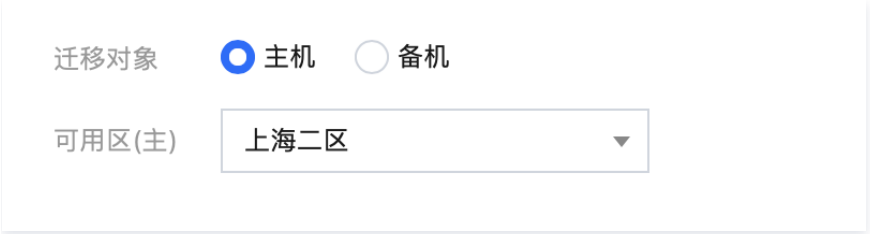
- 开启 ByPass：ByPass 模式下当前实例下所有流量均不会过防火墙，所有防火墙配置将失效。建议在调试时使用，开启后预计1分钟内生效。调试完成后请手动关闭 ByPass 模式，如需更多帮助请 提交工单 。

> ⚠ **注意：**
> 开启 ByPass 模式可能会出现以下影响：
> 1. 切换路由过程会有几秒闪断。
> 2. 存量长连接会受影响，需要自动重试新建连接。

- 重启实例：我们会优先重启防火墙备机，重启完成会进行主备切换再重启防火墙主机，主机重启完成后会再次进行主备切换。整个过程预计持续10分钟左右，网络可能会出现轻微抖动，您无法对操作或修改防火墙配置，建议在业务低峰期操作。
- 切换主备：防火墙采用互为主备的方案，即工作的实例为主实例；您可以选择是否切换至备用防火墙实例。切换过程预计耗时2-10s左右，网络可能会出现轻微抖动。
- 拨测设置：设置公网拨测地址。

a. 防火墙会采用定时拨测的方式来探测 NAT 边界防火墙绑定 EIP 的存活情况，因此需要您指定可达的公网 IP 地址用于拨测。
b. 您最多可以同时添加 5 个IP 地址。当存在设置的出口绑定地址不可达后，防火墙会启用高可用机制切换至备用 EIP。

- 开启透明模式：透明模式下当前防火墙实例对网络流量仅做转发，相关访问控制功能或入侵防御功能不会生效。建议在调试时使用，开启后预计1分钟内生效。调试完成后请手动关闭透明模式，如需更多帮助请 提交工单 。
- 迁移可用区：您可以选择将当前主机或备机进行可用区迁移。迁移过程预计持续2-5分钟左右，可能会进行主备切换等操作，网络会发生抖动，建议在业务低峰期操作。



相关信息

- 如需对所持有的公网 IP 以及关联的云上资产，配置对应的防火墙开关，可参见 互联网边界防火墙开关 进行操作。
- 如需自动探测 VPC 信息与互通关系，并在每一对互通的 VPC 间，建立云防火墙开关，可参见 VPC 间防火墙开关 进行操作。
- 已绑定外网 IP 的主机，如需直接通过外网 IP 访问，请参见 调整 NAT 网关和 EIP 的优先级 文档。
- 如遇到 NAT 边界防火墙相关问题，可参见 NAT 边界防火墙 文档。

VPC 边界防火墙

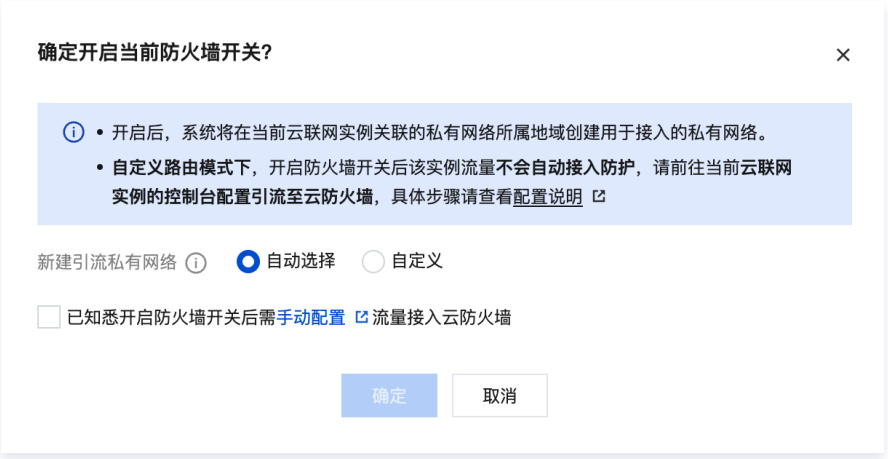
最近更新时间：2025-07-01 16:12:11

云防火墙提供集群模式的 VPC 边界开关功能，在 VPC 边界开关页面，可自动探测到您所持有的云联网实例，并为您配置对应的防火墙开关。
您可以登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **防护对象** > **VPC 边界**，进行集群模式的 VPC 边界防火墙的配置。

> **说明：**
> VPC 边界防火墙开关当前**仅支持自定义路由接入模式**，在开启防火墙开关后该实例流量不会自动接入云联网实例流量，请前往当前云联网实例的控制台配置引流至云防火墙，具体步骤请参见 自定义路由配置指引 。配置成功后当前云联网实例的流量将经过防火墙，届时访问控制规则、入侵防御功能将对其生效，流量日志也会生成。

防火墙开关

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **防护对象** > **VPC 边界**。
2. 在 VPC 边界开关页面，在防护对象列中找到需要防护的云联网实例。
3. 单击防火墙开关列的并选择新建引流私有网络方式。



4. 确定开启后，云防火墙将在对应云联网实例关联的私有网络所属地域创建用于接入的私有网络。
5. 当前防护对象的接入模式为“自定义路由”时，开启防火墙开关后需要前往当前云联网实例的控制台配置引流至云防火墙，具体操作请参见 自定义路由配置指引 。

> **说明：**
> - VPC 边界防火墙不支持在开启防火墙开关前预先配置路由表。您需要先开启防火墙开关，待云防火墙自动创建完成引流所需的私有网络后，方可进行路由表的配置操作。
> - 关闭防火墙开关后，当前云联网类型实例接入防火墙所使用的相关网络资产（如私有网络、子网）将被自动清除。当前防护对象的接入模式为“自定义路由”时，务必在关闭防火墙开关前，先手动在云防火墙控制台取消该云联网实例的接入，否则直接关闭开关可能导致网络中断。详细操作步骤请参见 配置说明 。

防火墙状态监控

VPC 边界防火墙状态监控支持统计各个 CCN 实例的带宽。
1. 在带宽配置面板右上角，单击**查看状态监控**。

2. 在状态监控–①VPC 边界防火墙界面中，可以基于②云联网实例名称对带宽监控维度进行筛选，也可以选择在③切换查看连接数，通过选择④时间范围修改统计维度。可以看到⑤监控曲线，也可以查阅⑥不同视角的监控数据。

> **注意：**
> 不同时间范围的统计的最小统计颗粒度不同，可能会与实际峰值有误差，建议以 腾讯云可观测平台 的数据或具体防护单元的统计数据为准。

主备模式与集群模式的区别

VPC 边界防火墙主备模式与集群模式版本的差异请参见下表。

对比维度	主备模式	集群模式
架构类型	单活架构	多活架构
升级影响	主备切换导致网络抖动	无感升级
运维复杂度	需用户管理主备实例	自动维护节点及升级
高可用性	主机故障时备机自动接管	多节点负载，单点故障无影响

DNS 防火墙开关

最近更新时间：2024-05-17 15:14:11

DNS 防火墙与 Private DNS 联合，对 VPC 出站域名访问提供实时管控、风险告警、拦截、自定义策略和全流量审计。无需更换 DNS 或部署代理，即开即用。

> **说明：**
> 当前功能内测中，当前版本仅部分地域支持，如需申请请 提交工单 与我们联系，内测结束时间以后续公告为准。

使用 DNS 防火墙前准备

1. DNS 防火墙必须使用由 Private DNS 提供的默认 DNS 地址：183.60.83.19和183.60.82.98，如果您的 DNS 地址非上述 DNS 则无法使用 DNS 防火墙，建议使用 NAT 边界防火墙接入 DNS 流量防护。
2. DNS 防火墙仅防护 VPC 的出站域名访问流量，对入站场景及 Public DNS 解析均不涉及，请确认符合业务需求场景。

开启 DNS 防火墙开关

登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关 > DNS 开关**，进入 DNS 防火墙开关页面。在下面的开关列表中您可以看到基于您的 VPC 资产的 DNS 开关列表，选择您想要开启的 VPC 资产，单击右侧开关打开即可。开启对网络无影响。

查看 DNS 请求频率监控

1. 在状态监控面板右上角，单击图标。

2. 在新的窗口中，可以查看指定 VPC 的请求频率曲线或部分 IP 的具体监控指标。

状态监控
DNS防火墙
全部VPC
近1小时
近24小时
近7天
1个月
1. 云防火墙会持续监控您的DNS请求频率并统计请求总量；
2. 您可以实时关注DNS的请求频率并配置相应的监控告警策略。
峰值请求频率 | 全部VPC
1010 Qps
累积请求次数 5.9 万次
IP地址
资产ID/名称
关联VPC
峰值请求频率
累计请求次数
开关状态
操作
1010
59172
关闭
查看开关

自定义路由配置指引

最近更新时间：2025-04-27 10:13:21

云联网实例接入云防火墙

步骤1：创建自定义路由模式实例

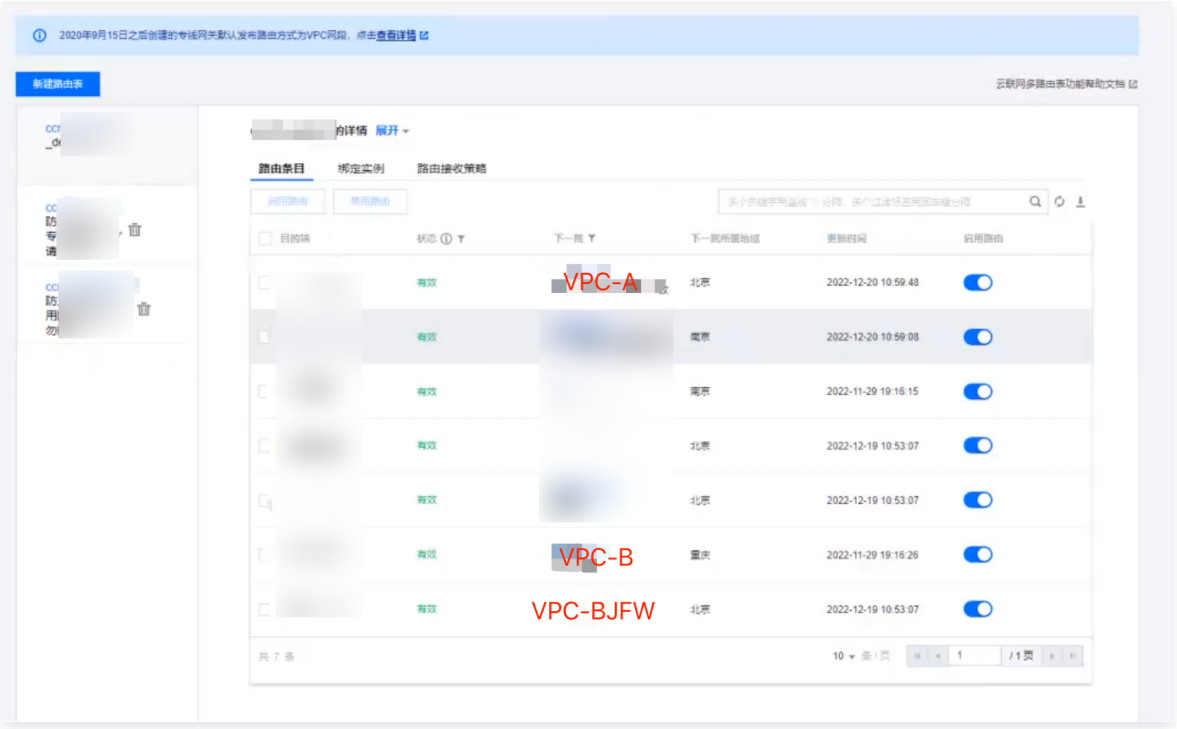
参考 VPC 边界防火墙，打开目标云联网实例的防火墙开关，其中接入模式选择自定义路由。

步骤2：配置引流路由

当前操作目的是将用户需要防护的业务 云联网实例 通过防火墙网关引流至云防火墙。

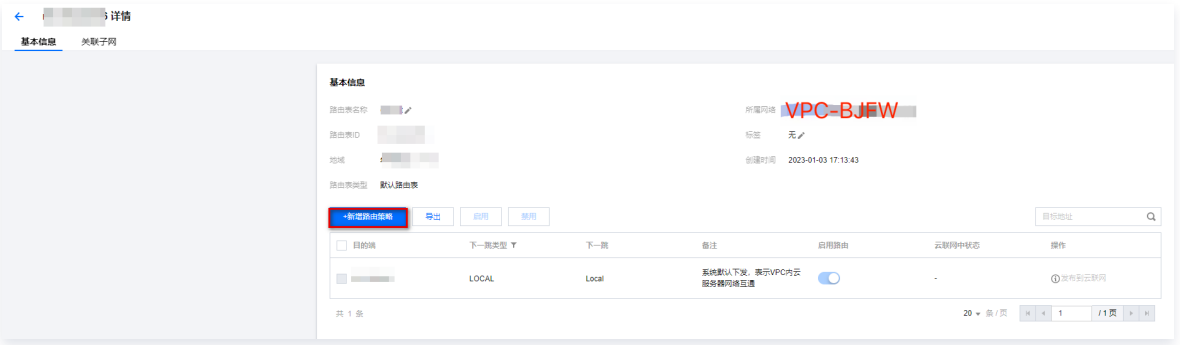
1. 前往打开 VPC 边界防火墙时选择的云联网实例的控制台，查看自定义路由模式关联的云联网实例详情。
2. 确认防火墙引流 VPC 和相关路由表已经创建，若未创建请等待实例创建完成或 提交工单 联系我们。
3. 查看默认路由表页面，确定需要接入的业务 VPC 及防火墙引流 VPC。

> **说明：**
> 本文以北京业务 VPC：VPC-A；重庆业务 VPC：VPC-B；北京地域防火墙引流 VPC：VPC-BJFW 举例来演示如何接入。

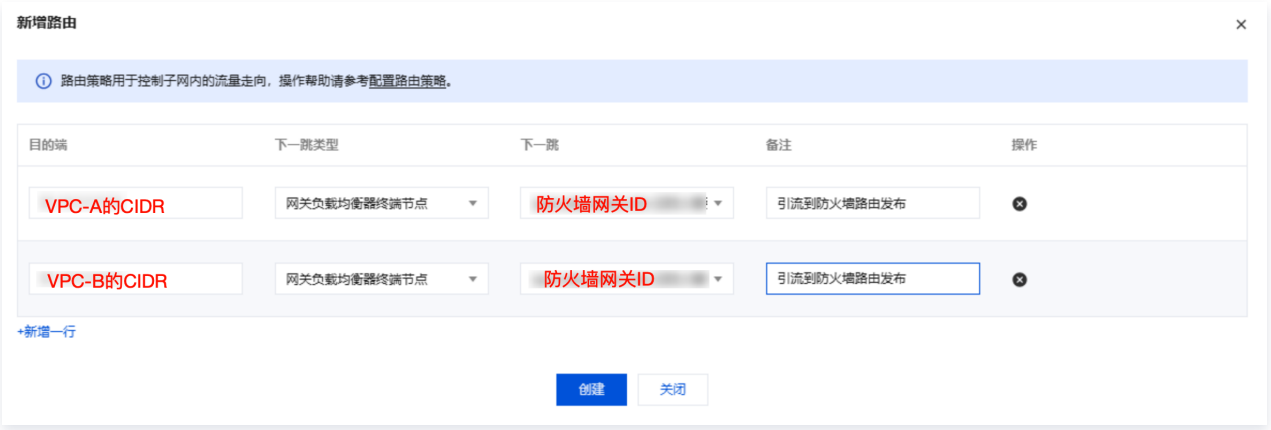


4. 前往**私有网络** > 路由表 页面，选择需要接入的防火墙引流 VPC，可以看到包含“防火墙 VPC 专用路由表_请勿删改”和“default”在内的路由表。选择“default”路由表编辑路由策略。

5. 单击**新增路由策略**，将业务 VPC 下一跳引流至防火墙。



目的端输入业务 VPC 的 CIDR，下一跳类型选择**网关负载均衡器终端节点**，下一跳选择**防火墙网关 ID**，备注可以自由填写。



> **说明：**
> 若有提示“指定 CIDR 形成 ECMP”时，需要先在默认路由表中停用相关业务路由。

6. 将新增路由发布到云联网，详情请参见 管理路由策略 。发布后可以在对应云联网中的默认路由表看到指定路由策略。

> **说明：**
> 因新路由策略与原路由策略冲突，原路由条目会失效，可以忽略。

步骤3：建立业务 VPC 互访路由表

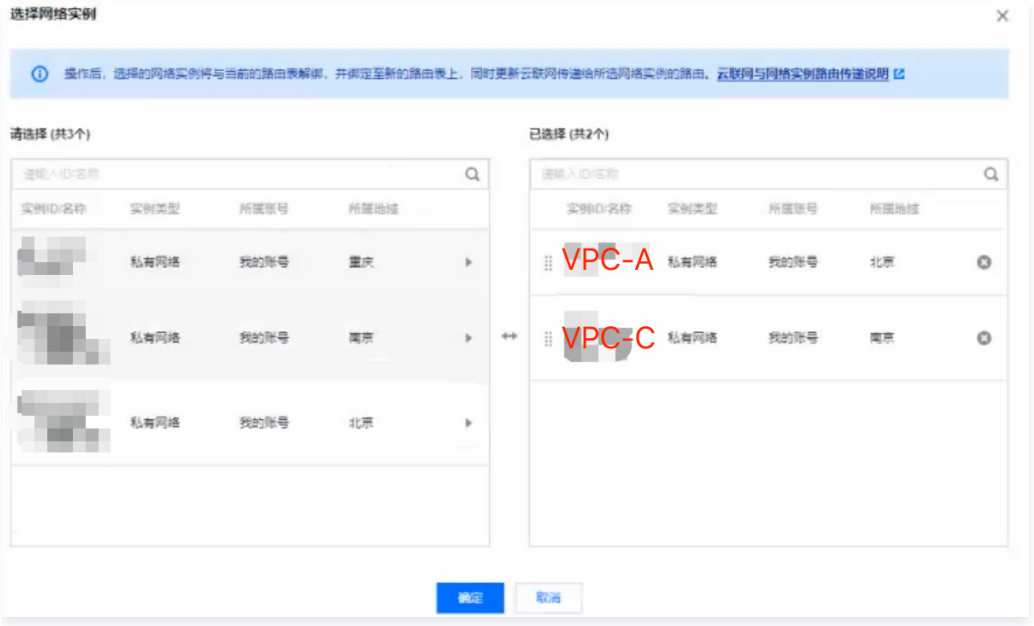
当前操作目的是为了将防火墙网络和用户的业务网络打通，实现网络互访。

1. 在 云联网页面 ，分别为每个引流至防火墙的业务 VPC 建立路由表。

2. 调整路由接收策略。在各个 VPC 的专属路由表中的**路由接收策略**中单击**添加网络实例**，将路由表自身所属 VPC 实例和互通 VPC 实例添加至路由表中。

> **注意：**
> 添加网络实例务必分为两个步骤，先添加自身 VPC 实例和不经过防火墙防护的 VPC 实例；再添加防火墙引流专用 VPC 实例。

例如：假设 VPC-C 是不需要接入防火墙实例的业务 VPC，则在 VPC-A 的路由表中应先添加 VPC-A，VPC-C 两个实例，添加成功后，重复上述操作再添加 VPC-BJFW 一个实例。



3. 检查各个 VPC 的专属路由表中路由条目是否符合预期。
4. 绑定网络实例。各个 VPC 的专属路由表的**绑定实例**单击**绑定网络实例**，将各个 VPC 专属路由表绑定至其对应的 VPC 实例，操作完成后网络会引流至防火墙。

> **注意：**
> 请务必确认路由无误后再绑定路由表，绑定后会立即生效。

步骤4：验证防火墙是否正常工作

1. 参考 日志审计 查看是否有流量日志。
2. 参考 日志审计 查看入侵防御是否正常。
3. 配置内网间规则，检查是否正常命中。

至此防火墙已正常工作，如果您的网络结构较为复杂或涉及专线场景，请 提交工单 咨询详细路由配置方案；如果您有更多疑问也欢迎 提交工单 联系我们。

云联网实例取消接入云防火墙

> **注意：**
> 请务必确认云联网实例取消接入云防火墙后，再关闭对应 VPC 边界防火墙开关，否则将会造成网络中断。

1. 前往需要关闭 VPC 边界防火墙的云联网实例的控制台，查看自定义路由模式防护对象关联的云联网实例详情。
2. 除了防火墙专用 VPC 之外，将所有网络实例绑定到接入云防火墙之前使用的路由表中。
   2.1 选择接入云防火墙之前使用的路由表，一般为_default_rtb表。

   2.2 选择除防火墙专用之外的所有实例。

   2.3 确认路由，完成取消接入云防火墙。

3. 检查网络正常后，在云防火墙控制台关闭当前云联网实例对应的防火墙开关。

防火墙引擎升级

最近更新时间：2025-04-14 16:41:31

NAT 边界防火墙与 VPC 间防火墙为私有化部署，其引擎由租户独享，故需要用户手动更新引擎，以下为升级操作指引。

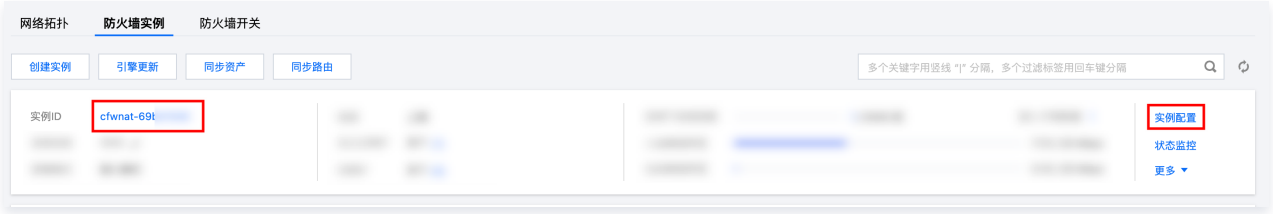
查询可升级的防火墙实例

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **NAT 边界开关/VPC 间开关**。
2. 在防火墙实例页面，单击**引擎更新**，查看最新版本引擎及可升级的实例。

3. 我们会默认选中最新稳定版本，如果存在可升级防火墙实例下方升级选项将可选。

4. 您也查看具体实例的引擎版本及是否可升级。

   单击对应防火墙实例 ID 或实例配置，呼出防火墙实例详情页面。



5. 比对当前引擎版本与引擎更新动态给出的版本列表是否可升级，如果可升级引擎版本右侧会出现⬆标志。

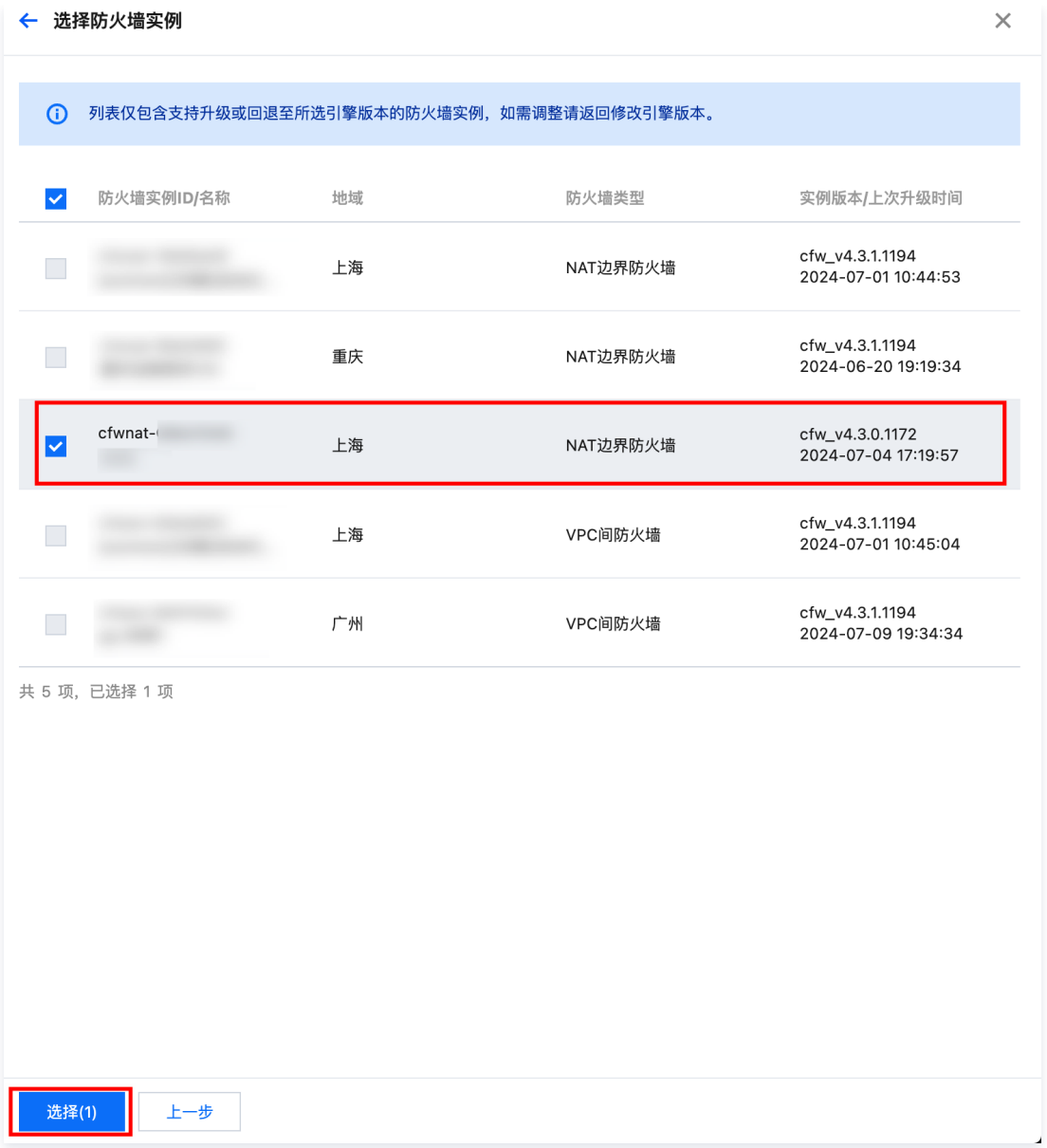
升级防火墙引擎版本

1. 参照 上述章节 进入引擎升级页面，在图示位置选择需要升级的引擎版本。

> **说明：**
> 预览版为最新引擎版本，包含了最新的特性功能和缺陷修复；稳定版为经过现网长时间稳定性验证后的版本，一般落后预览版一个大版本。
> 我们推荐您及时将引擎更新至最新稳定版本，版本详情参见 引擎更新动态 。

2. 选择需要升级的引擎实例。
   - **一键升级**：选择此选项后，将自动识别所有地域当前版本的防火墙引擎实例，并升级至所选版本。
   - **自定义升级**：可以自定义选择实例进行升级，单击**点击选择/选择实例**，进入实例选择界面。

3. 在实例选择页面，选择需要升级的实例，单击**选择**。



4. 单击**确认升级**，即可发起升级任务。

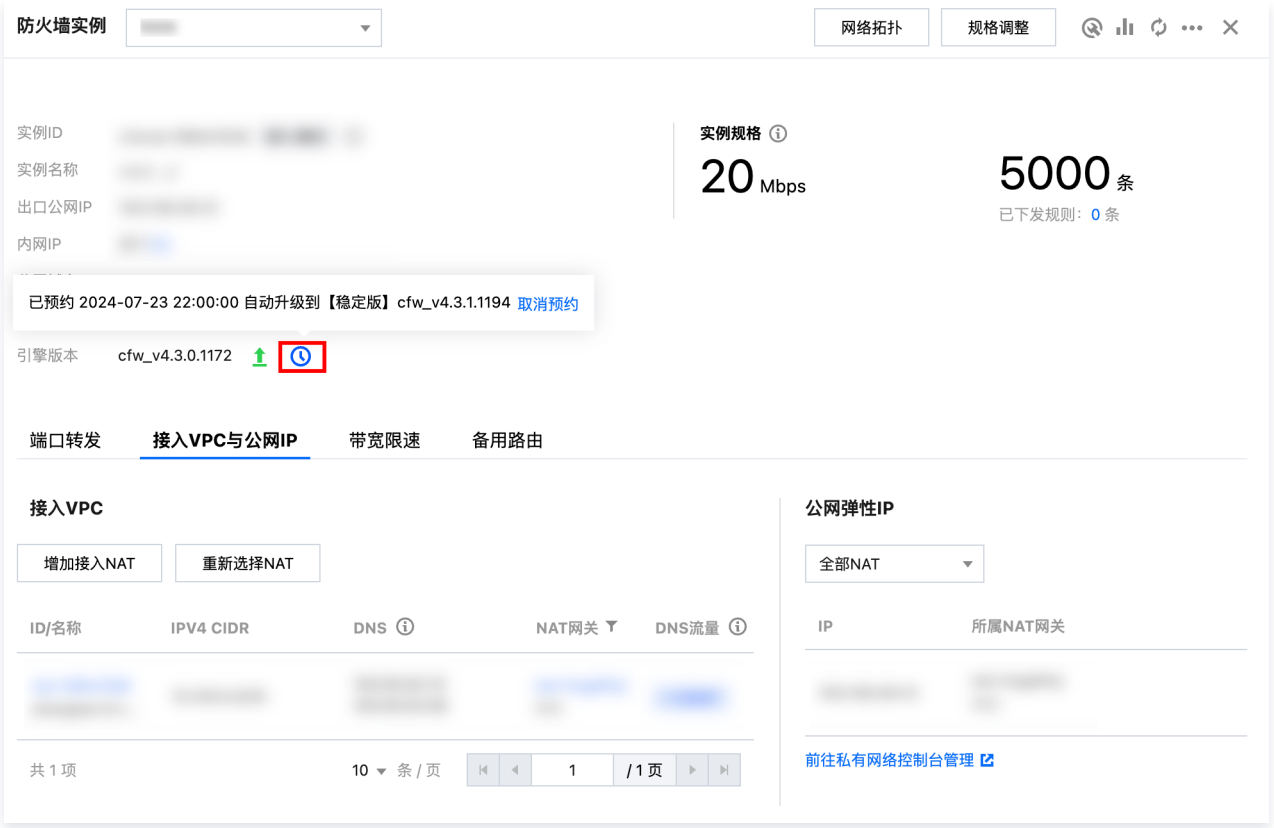
> **说明：**
> - 升级过程可能需要若干分钟，期间无法操作防火墙开关和规则；升级完成后，会自动复原开关和规则的状态。
> - 升级过程会先升级备机再升级主机，升级期间会触发主备切换操作，网络可能会略微抖动，业务不会断联。建议在业务低峰期进行升级操作。

预约时间升级

1. 完成上述章节1、2步后，在图示位置单击**选择预约时间**。

2. **确认升级任务状态。**

   进入对应防火墙实例页面，您可以在图示引擎版本处看到预约升级任务，您可以通过单击取消预约或重新执行引擎升级操作来取消本次预约。


防火墙实例
网络拓扑
规格调整
实例ID
实例名称
出口公网IP
内网IP
实例规格
20 Mbps
5000 条
已下发规则：0 条
已预约 2024-07-23 22:00:00 自动升级到【稳定版】cfw_v4.3.1.1194 取消预约
引擎版本
cfw_v4.3.0.1172
端口转发
接入VPC与公网IP
带宽限速
备用路由
接入VPC
增加接入NAT
重新选择NAT
ID/名称
IPV4 CIDR
DNS
NAT网关
DNS流量
共 1 项
10 条 / 页
1
/ 1 页
公网弹性IP
全部NAT
IP
所属NAT网关
前往私有网络控制台管理

防火墙引擎地域迁移

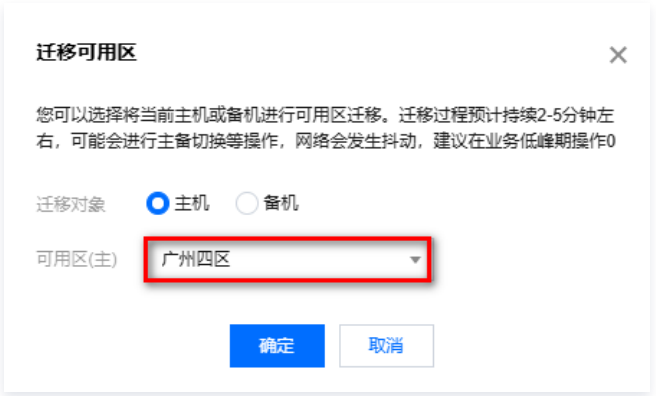
最近更新时间：2024-11-14 17:38:22

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关**。
2. 根据实例类型，切换至 **NAT 边界开关**或 **VPC 间开关**。

3. 在防火墙实例页签，选中需要迁移可用区的引擎实例，单击**更多** > **调试工具** > **迁移可用区**。

4. 在迁移可用区弹窗中，为**备机**选择一个与**主机**不同的可用区，单击**确定**，完成操作。

> **注意：**
> 主机迁移可用区过程中，会出现主备切换导致网络抖动，建议在非业务时间进行主机迁移；备机迁移不会产生影响。



VPC 边界防火墙开关（主备模式）
概述

最近更新时间：2024-10-17 20:59:31

操作场景

云防火墙开关提供 VPC 间防火墙开关功能，通过建立防火墙来承载不同 VPC 之间的访问流量，提供访问控制规则和日志审计系统。
当前版本的 VPC 间防火墙支持专线网关的防护，基于防火墙实例支持 CCN 多路由云联网模式，专线网关通过云联网与云上 VPC 资产建立连接，那么VPC间防火墙支持对这部分流量进行检测。
本文将介绍如何在 VPC 间开关页面，创建防火墙、查看带宽使用情况、规格信息以及查看网络拓扑和防火墙开关等操作。

架构简介

在系统使用此功能前，您需要先大概了解下 VPC 间防火墙的构成。
1个 VPC 间防火墙由多个防火墙实例组成，每个防火墙实例负责接入不同的 VPC 并打通与防火墙之间的网络连接。

VPC 间防火墙本质是通过修改 VPC 的路由实现将流量牵引至防火墙。防火墙实例之间是否互通，取决于不同实例之间接入的 VPC 是否**存在可达路由通路**，防火墙不会打通基础网络。防火墙打通网络的方式可通过修改私有网络的路由表下一跳或云联网多路由表实现。

VPC 间防火墙的异常场景说明

- VPC 间防火墙在开启和关闭开关时，涉及后台自动修改您的路由策略，导致**在一个极短的时间内会出现网络闪断**，为不影响您的业务，请您合理安排操作 VPC 间防火墙开关的时间。如果需要进行批量或频繁的开关操作，建议在业务流量较小的深夜进行。

  > **说明：**
  > 互联网边界防火墙的开关不存在类似问题。

- VPC 间防火墙开关建立在 VPC 间的对等连接（或云联网）之上，若您变更（或删除）了对等连接（或云联网）的配置，则防火墙开关也会自动对应变更（或删除）。为了不影响您的业务，云防火墙只会对状态为关闭的开关立即执行变更（或删除）。

  > **说明：**
  > 若您的云上资产有所变更（或删除），互联网边界防火墙开关会在短时间内（5分钟左右）自动同步。

- 若 VPC 间没有正在启用的路由，则防火墙开关无法开启。

  > **说明：**
  > - 如需配置对等连接路由，请参见 配置指向对等连接的路由 。
  > - 如需配置云联网路由，请参见 路由概述 。

- 云防火墙开关开启状态下，**在 私有网络控制台 手动变更对应 VPC 路由表属于高危操作**，由于云防火墙无法同步路由的变更，可能导致防火墙失效，网络连接中断。
- 云防火墙开关关闭状态下，您可以根据需要切换 VPC 间的其他对等连接（或云联网）路由，但**请勿启用备注信息为“防火墙”的路由**，否则将导致网络连接中断，防火墙开关故障。

相关信息

- 如需对所持有的公网 IP 以及关联的云上资产，配置对应的防火墙开关，可参见 互联网边界防火墙开关 进行操作。
- 如需对内网资产进行流量管控与安全防护，或基于 SNAT、DNAT 进行的网络流量转发，可参见 NAT 边界防火墙开关 进行操作。

- 如遇到 VPC 间防火墙相关问题，可参见 VPC 间防火墙 文档。

新建 VPC 边界防火墙（主备模式）

最近更新时间：2025-06-18 09:47:32

私有网络模式

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **VPC 间开关**。
2. 在 VPC 间开关页面，单击**防火墙实例**，进入到防火墙实例页面，单击**创建防火墙**。

3. 在新建 VPC 间防火墙弹窗中，输入实例名称，选择**私有网络模式**，单击**下一步**。

参数说明：

- 实例名称：创建防火墙实例时自定义的名称。
- 模式：
  - 私有网络模式：选择私有网络 VPC 接入防火墙，通过修改相关私有网络的路由表，来实现路由牵引。
  - 云联网模式：选择云联网 CCN 接入防火墙（需要支持多路由表模式），通过修改云联网路由表，来实现路由牵引。
  - SASE 模式：功能限时内测中，如需使用请 提交工单 。
  - 私有网络模式(CDC)：与私有网络模式一致，仅 CDC 环境可用。

4. 填写防火墙实例名称和地域，配置灾备信息，设置防火墙实例带宽规格和接入网络，单击**下一步**。若实例数量不满足需求可单击右侧创建多个防火墙实例。

参数说明：

- 地域：接入防护的 VPC 所属的地域。
- 异地灾备：VPC 间防火墙支持异地灾备，通过勾选来开启。
- 可用区：根据需求选择合适的可用区。
- 实例带宽：单实例目前最小1Gbps，最大20Gbps（控制台自行配置最大支持5Gbps，超过请 提交工单 评估），支持 升级扩容。如果不满足最大带宽可创建多个防火墙实例分流。但请注意，每个防火墙实例有其自身吞吐上限，多个防火墙实例请确认单实例在吞吐上限内。
- 实例接入：单击**接入网络**，根据需要接入的 VPC 的地域分实例，选择所需 VPC，单击**确定**。

> **注意：**
> - 1个 VPC 仅可以接入1个实例。
> - 防火墙无法进行基础网络的打通，接入网络之前，请确认 VPC 间已经创建对等链接/云联网，如果 VPC 之间没有建立连接，则接入不生效，不会有防火墙开关。
> - 每个防火墙实例仅可接入同地域下的 VPC，每个实例最多可接入10个 VPC，支持同地域下创建多个防火墙实例。建议提前按照地域规划需要接入的 VPC，再创建防火墙实例并进行网络接入。

5. 配置创建引流子网方式、防火墙 VPC、路由模式，确认无误后单击**创建**即可。

> **说明：**
> 完成配置，创建过程需要等待若干分钟，请耐心等待。

参数名称	说明
创建引流子网方式	云防火墙会在您所接入的VPC中新建24网段的子网，用于将流量牵引至防火墙，您可以选择不同的创建子网的方式。引流子网完成防火墙创建后不可修改。 • 自有网段优先：云防火墙会在您所选的 VPC 内自动选择空闲子网网段；当 VPC 内无子网配额时，我们会使用所选 VPC 的扩展网段。

	• 扩展网段优先：云防火墙会优先使用空闲的 VPC 保留的扩展网段，该模式下不会占用所选 VPC 子网配额。其中，扩展网段是指私有网络中的辅助网段，详情可参见 私有网络-编辑 IPv4 CIDR 。 • 自定义：您可以自定义供防火墙使用的子网网段，请注意必须为24网段；自定义网段必须属于当前 VPC 的 CIDR，例如192.168.0.0/24。
防火墙 VPC	用来打通防火墙实例之间的网络通信，需要在所选 VPC 的所在地域各新建一个防火墙专用 VPC。 • 自动选择：防火墙会自动创建一个与接入 VPC 不冲突的20网段的 VPC。 • 自定义：请输入一个与规划网络不冲突的20段 VPC，例如192.168.1.0/20。
路由模式	防火墙开关的引流方案，不同的网络互通方式决定了防火墙开关和路由引流的模式不同，建议根据业务网络模式选择。 • 单点互通：适用于 VPC 数量较少，网络结构简单的拓扑；开关模式为 VPC 到 VPC，该模式下每个 VPC 之间的可达通路均会生成一个防火墙开关。 • 多点互通：适用于 VPC 数量较多，网络拓扑简单，如星型网络拓扑等；开关模式为单 VPC，该模式下 VPC 之间的访问会经过两个开关控制。 • 全互通：适用于 VPC 数量较多，网络拓扑复杂，如网状网络拓扑等；开关模式为全部 VPC，该模式下仅会有一个防火墙开关用于控制全部 VPC 路由。 • 自定义路由：您可以参考文档 自定义路由配置指引，在完成创建防火墙后自行配置路由，该模式下不会存在防火墙开关。 注意：选择多地域后仅支持自定义路由，具体路由模式是否可用请以控制台为准。

云联网模式

> **注意：**
> 自2023年07月01日起，云联网服务将对网络实例和入流量处理进行收费，云防火墙需要在您接入的云联网实例中新建一个防火墙专用 VPC 用于引流，可能会产生一定费用，详情请参见 云联网商业化公告 。

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关 > VPC 间开关**。
2. 在 VPC 间开关页面，单击**防火墙实例**，进入到防火墙实例页面，单击**创建防火墙**。

3. 在新建 VPC 间防火墙弹窗中，输入实例名称，选择**云联网模式**，单击**下一步**。

4. 单击**点击选择**，根据提示选择需要加入 VPC 防火墙的云联网实例，单击**确定**。

> **注意：**
> - 需要云联网实例支持多路由表模式，如未满足请先联系云联网开启多路由表功能。
> - 云联网模式支持在指定地域创建 VPC 间防火墙。
> - 云联网模式一个防火墙仅能绑定一个云联网实例。

5. 选择完云联网实例后，下方会自动根据云联网接入的 VPC 生成可选地域，若勾选地域则会在所选地域创建1个防火墙实例。您可以配置防火墙实例名称、是否异地灾备以及实例带宽规格，单击**下一步**。

参数说明：

- 地域：接入防护的 VPC 所属的地域。

  > **说明：**
  > - 若仅勾选一个地域部署防火墙实例，所有开启了防火墙开关的 VPC 间流量都会经过该地域的防火墙实例，适合星形拓扑结构的业务网络。
  > - 若选择全部地域部署防火墙实例，开启了防火墙开关的 VPC 间流量都会经过本地域的防火墙实例，适合网状拓扑结构的业务网络。
  > - 选择多地域后仅支持自定义路由。

- 异地灾备：VPC 间防火墙支持异地灾备，通过勾选来开启。
- 可用区：根据需求选择合适的可用区。
- 实例带宽：单实例目前最小1Gbps，最大20Gbps（控制台自行配置最大支持5Gbps，超过请 提交工单 评估），支持 升级扩容 。如果不满足最大带宽可创建多个防火墙实例分流。

  > **注意：**
  > 每个防火墙实例有其自身吞吐上限，多个防火墙实例请确认单实例在吞吐上限内。

6. 配置新建引流私有网络、路由模式，确认无误后单击**创建**即可。

> **说明：**
> 完成配置，创建过程需要等待若干分钟，请耐心等待。

参数名称	说明
新建引流私有网络	云防火墙会在您所选的云联网实例中新建20网段的私有网络，用于将流量牵引至防火墙，您可以选择不同的创建私有网络的方式。 • 自动选择：云防火墙会自动探测空闲的20段 VPC 网段，用于防火墙引流 • 自定义：您可以自定义供防火墙使用的私有网络网段，请注意必须为20网段。例如192.168.1.0/20 注意： 自2023年07月01日起，云联网服务将对网络实例和入流量处理进行收费，云防火墙需要在您接入的云联网实例中新建一个防火墙专用 VPC 用于引流，可能会产生一定费用，详情请参见 云联网商业化公告 。
路由模式	防火墙开关的引流方案，不同的网络互通方式决定了防火墙开关和路由引流的模式不同，建议根据业务网络模式选择。 • 单点互通：适用于 VPC 数量较少，网络结构简单的拓扑；开关模式为 VPC 到 VPC，该模式下每个 VPC 之间的可达通路均会生成一个防火墙开关。 • 多点互通：适用于 VPC 数量较多，网络拓扑简单，如星型网络拓扑等；开关模式为单 VPC，该模式下 VPC 之间的访问会经过两个开关控制。 • 全互通：适用于 VPC 数量较多，网络拓扑复杂，如网状网络拓扑等；开关模式为全部 VPC，该模式下仅会有一个防火墙开关用于控制全部 VPC 路由。 • 自定义路由：您可以参考文档 自定义路由配置指引 ，在完成创建防火墙后自行配置路由，该模式下不会存在防火墙开关。 注意：选择多地域后仅支持自定义路由，具体路由模式是否可用请以控制台为准。

实例规格

VCP 间防火墙实例规格档位表。

说明：
- VPC 间防火墙实例规格与内网间规则列表配额互相独立，不涉及计费逻辑，无法额外单独扩容，仅能通过提升实例规格实现。您每在控制台配置一条 ACL，我们会自动按照下发公式帮您转换为特定规则，并自动识别访问源和访问目的，下发到指定 VPC 间防火墙实例上。
- 下发公式：下发规则数 = 源地址个数 × 目的地址个数 × 端口个数 × 协议个数。
- VPC 间防火墙实例规格决定了每个 VPC 间防火墙实例能承载的最大 ACL 规则数量，当 ACL 下发数量过多时可能会导致引擎出现不稳定的情况。
- 为了避免给您的业务造成影响，我们建议您根据每个实例的规格和下发规则数合理优化规则，减少冗余规则的占比，提升引擎稳定性。

规格档位	最低带宽/Mbps	最高带宽/Mbps	并发连接数/个	规则数配额/条
1	100	1,023	130,000	5,000（此档位不包含入侵防御功能）
2	1,024	1,300	250,000	20,000
3	1,301	4,095	300,000	40,000
4	4,096	6,143	600,000	60,000

5	6,144	10,239	1,000,000	120,000
6	10,240	102,400	2,000,000	200,000

查看 VPC 边界防火墙（主备模式）

最近更新时间：2025-04-17 19:17:42

查看状态监控

VPC 间防火墙状态监控支持统计防火墙整体带宽和各个实例的带宽，可以通过多个入口查询。

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **VPC 间开关**。
2. 在 VPC 间开关页面，支持如下三种方法呼出监控面板：
   - 单击状态监控右上角的，或单击**防火墙峰值带宽**与**单实例峰值带宽**面板可快速呼出监控面板。

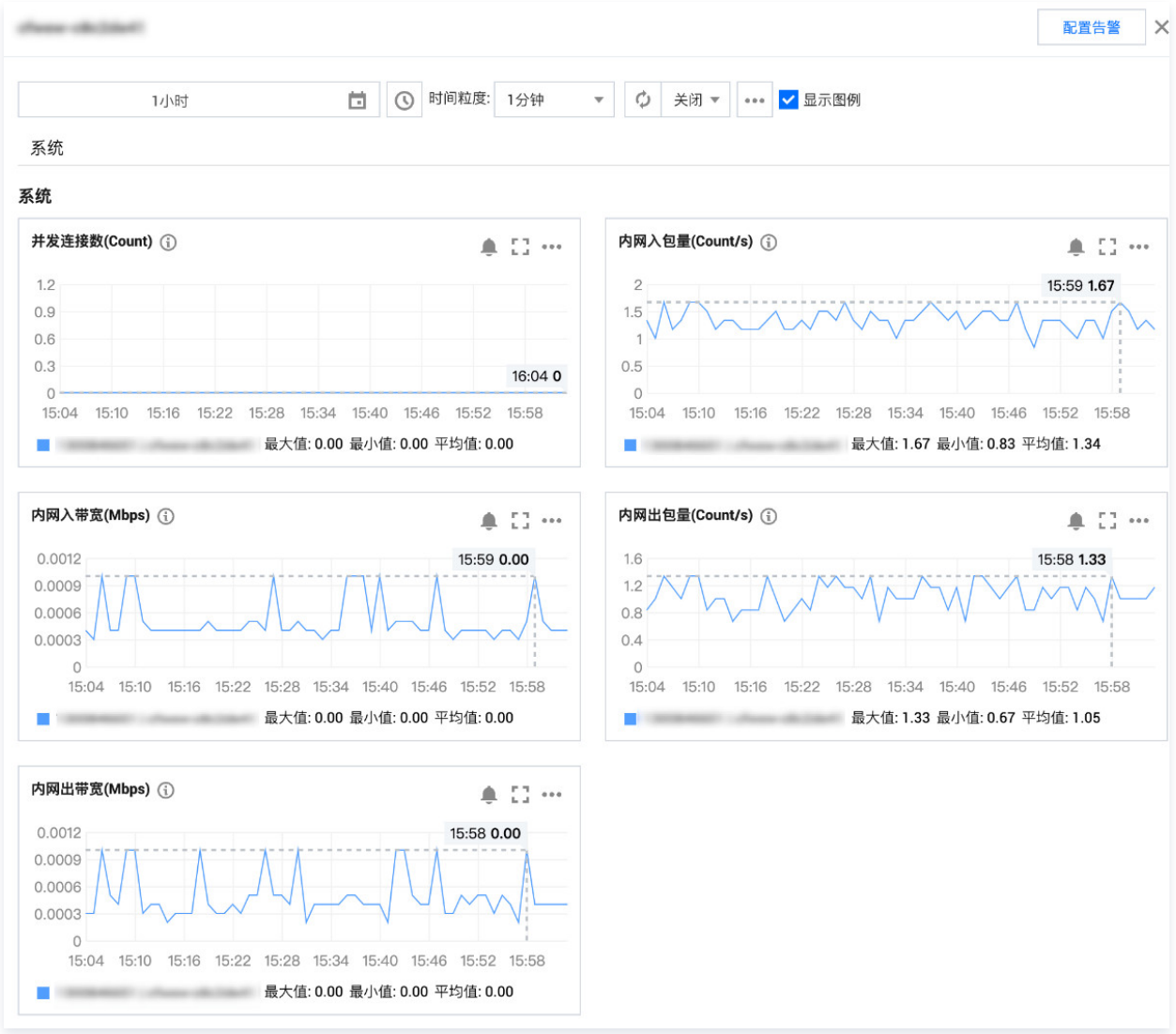
   - 单击**防火墙实例**，选择所需防火墙，单击**操作** > **带宽监控**，可快速呼出监控面板。

   - 单击**防火墙实例**，选择所需防火墙实例，单击**状态监控**，可快速呼出监控面板。

3. 在监控面板中，可以基于①防火墙名称或②防火墙实例名称对监控维度进行筛选，也可以通过选择③时间范围修改统计维度。可以看到带宽的④监控曲线，也可以查阅防火墙或实例下所属开关的⑤峰值带宽数据。

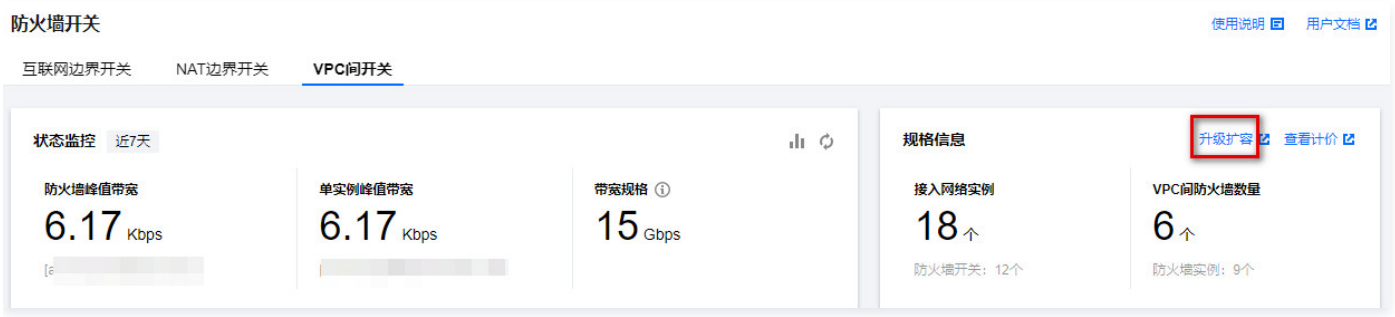
> **注意：**
> 不同时间范围的统计的最小统计颗粒度不同，可能会与实际峰值有误差，建议以 腾讯云可观测平台 的数据或具体防护单元的统计数据为准。

4. 在监控面板中， 单击**查看监控指标**呼出腾讯云可观测平台的侧边栏，查看防火墙实例的全部监控指标数据，包括并发连接数、内网入包量、内网出包量、内网出带宽、内网入带宽。您也可以前往 腾讯云可观测平台控制台 查看详细指标或配置相关告警。



查看规格信息

在 防火墙开关页面 的规格信息模块中，可以查看规格信息，包括接入网络实例和 VPC 间防火墙实例。单击规则信息右上角的**升级扩容**，可以跳转到扩容界面。默认规格下，企业版用户最多支持创建 1个 VPC 间防火墙，旗舰版用户支持 3个 VPC 间防火墙；若需扩展容量，可通过升级版本或扩容资源实现。



管理 VPC 边界防火墙（主备模式）

最近更新时间：2025-02-25 14:29:02

VPC 间防火墙创建完成后，您可以管理 VPC 间防火墙或防火墙实例。

查看概况

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **VPC 间开关**。
2. 在 VPC 间开关页面，单击**防火墙实例**，进入到防火墙实例页面，可以查看已经创建好的防火墙和其部署的防火墙实例信息。

> **说明：**
> 实例规格：当前防火墙实例的带宽上限和下发规则数上限，详情您可以参考 实例规格 。

查看关联开关

在防火墙实例页面，单击**开关数量**，跳转至防火墙开关页面，可自动筛选出当前防火墙关联的开关。

配置实例

1. 在防火墙实例页面，鼠标悬浮至需要配置的 VPC 间防火墙右侧的**操作**，选择**配置实例**。

2. 支持调整创建时的初始配置，包含防火墙实例名称、实例的规格以及每个实例接入的网络实例；也可以新增 VPC 间防火墙实例。

版权所有：腾讯云计算（北京）有限责任公司

3. 如果有新增接入的 VPC，将会自动根据创建 VPC 间防火墙时的网络配置执行；如果选择了自定义创建引流子网方式，还需要手动填写新增 VPC 的子网 CIDR。

> **注意：**
> 防火墙网络配置不支持修改。

销毁 VPC 间防火墙

在防火墙实例页面，鼠标悬浮至需要配置的 VPC 间防火墙右侧的**操作**，选择**销毁防火墙**，二次确认后即可。

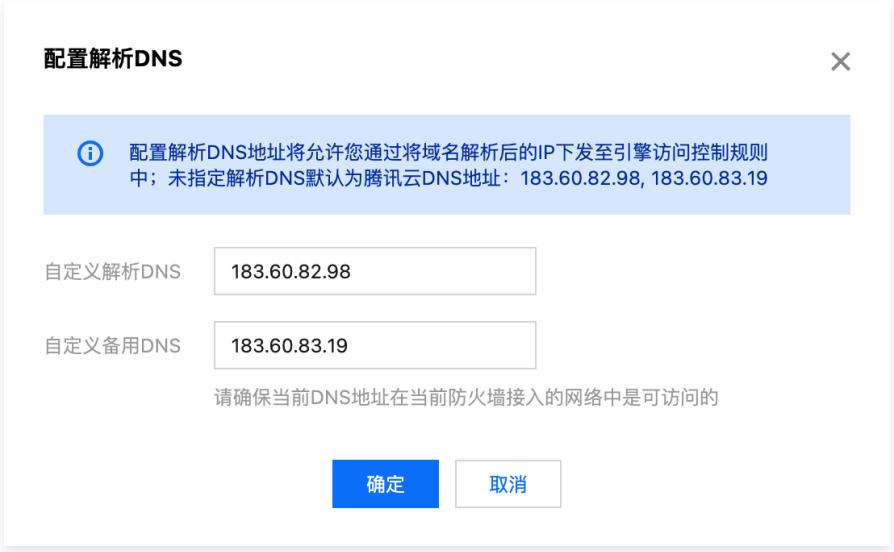
> **注意：**
> 若您选择了自定义路由请确认已手动恢复路由。

配置解析DNS

1. 在防火墙实例页面，鼠标悬浮至需要配置的 VPC 间防火墙右侧的**操作**。

2. 单击**配置解析 DNS**，可以配置用于域名解析类型的访问控制规则的自定义 DNS 解析服务器地址。
3. 在配置解析 DNS 窗口中，填写相关参数，单击**确定**保存。

> **说明：**
> 默认情况下，将使用腾讯云默认的 DNS 服务器地址，分别为183.60.82.98和183.60.83.19。如果您需要指定 DNS 服务器进行解析，请在下方填写。



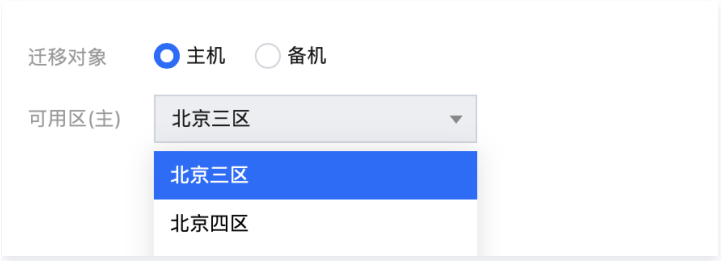
调试工具

在 VPC 间开关 > **防火墙实例**页面，选中所需实例，单击**更多**，在下拉框中，单击**调试工具**。

- 开启 ByPass：ByPass 模式下当前实例下所有流量均不会过防火墙，所有防火墙配置将失效。建议在调试时使用，开启后预计1分钟内生效。调试完成后请手动关闭 ByPass 模式，如需更多帮助请 提交工单 。

> **注意：**
> 开启 ByPass 模式可能会出现以下影响：
> 1. 切换路由过程会有几秒闪断
> 2. 存量长连接会受影响，需要自动重试新建连接。

- 重启实例：我们会优先重启防火墙备机，重启完成会进行主备切换再重启防火墙主机，主机重启完成后会再次进行主备切换。整个过程预计持续10分钟左右，网络可能会出现轻微抖动，您无法对操作或修改防火墙配置，建议在业务低峰期操作。
- 切换主备：防火墙采用互为主备的方案，即工作的实例为主实例；您可以选择是否切换至备用防火墙实例。切换过程预计耗时2-10s左右，网络可能会出现轻微抖动。
- 开启透明模式：透明模式下当前防火墙实例对网络流量仅做转发，相关访问控制功能或入侵防御功能不会生效。建议在调试时使用，开启后预计1分钟内生效。调试完成后请手动关闭透明模式，如需更多帮助请 提交工单 。
- 迁移可用区：您可以选择将当前主机或备机进行可用区迁移。迁移过程预计持续2-5分钟左右，可能会进行主备切换等操作，网络会发生抖动，建议在业务低峰期操作。



管理 VPC 边界防火墙实例（主备模式）

最近更新时间：2024-05-17 15:14:11

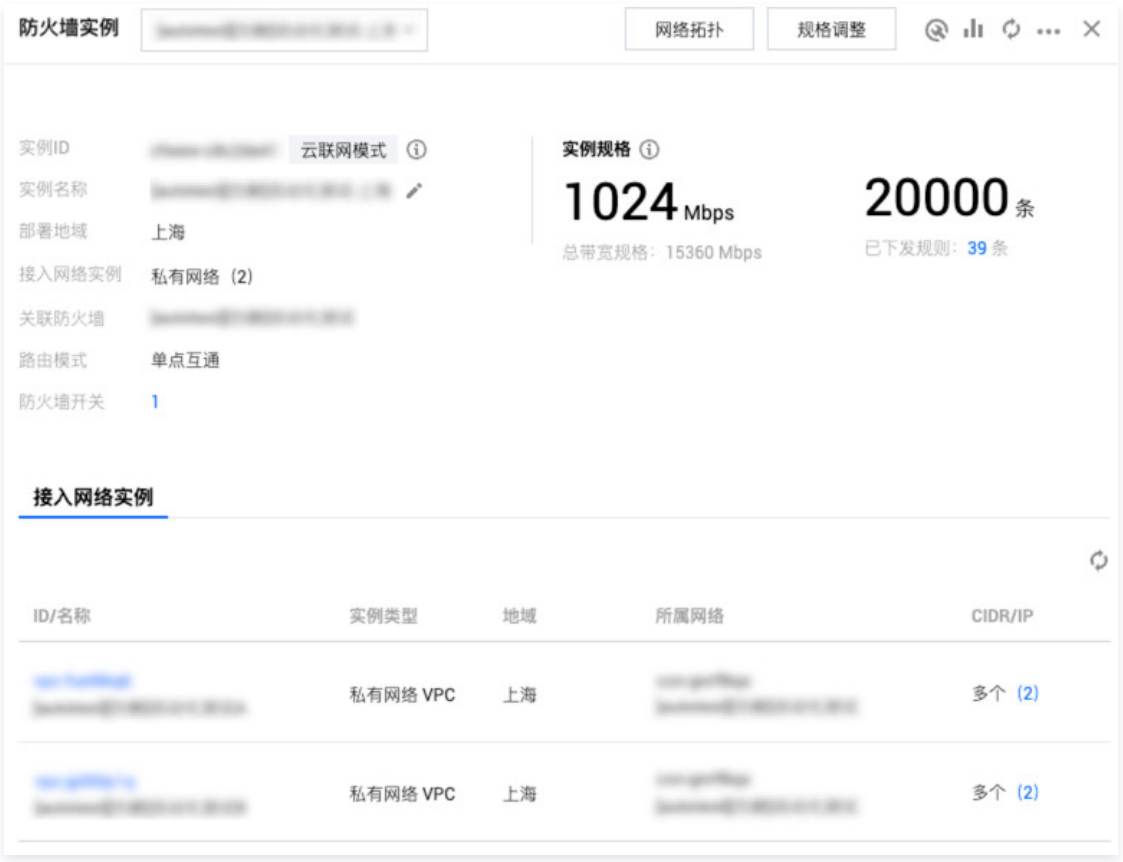
VPC 间防火墙创建完成后，您可以单独对 VPC 间防火墙实例进行管理。

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关 > VPC 间开关**。
2. 在 VPC 间开关页面，单击**防火墙实例**，进入到防火墙实例页面。

查看实例详情

1. 在防火墙实例页面，单击**防火墙实例 ID**或单击右侧的**实例详情**。

2. 在防火墙实例页面，可以查看实例的相关配置详情。



查看关联开关

在防火墙实例页面，单击**更多 > 查看防火墙开关**，可以跳转至防火墙开关页面，并自动筛选出当前防火墙实例关联的开关。

说明：
防火墙实例关联开关取决于开关控制的流量是否会经过这个实例，一个开关可能属于多个实例。

销毁 VPC 间防火墙实例

销毁任意防火墙实例，需要关闭当前 VPC 间防火墙的全部开关。

1. 在防火墙实例页面，单击所属 VPC 间防火墙的**开关数量**。

2. 跳转至防火墙开关页面，单击**全部关闭**关闭当前防火墙全部开关。

3. 在防火墙实例页面，单击**更多 > 销毁实例**，二次确认后即会销毁当前防火墙实例。

说明：
销毁防火墙实例后，当前实例接入的 VPC 将会自动取消接入，已使用配额将归还。

重新选择接入实例

重新选择接入实例，需要关闭当前 VPC 间防火墙的全部开关。

1. 在防火墙实例页面，单击所属 VPC 间防火墙的**开关数量**。

2. 跳转至防火墙开关页面，单击**全部关闭**关闭当前防火墙全部开关。

3. 在防火墙开关页面，单击**更多 > 重新选择接入实例**，进入编辑 VPC 间防火墙页面。

> **注意：**
> - 当以私有网络模式接入 VPC 间防火墙，支持重新选择接入的 VPC 实例。
> - 云联网模式则接入云联网内的所有 VPC 实例，不支持重新选择。

4. 在弹窗中，选择需要重新接入的 VPC，单击**确定**。

ByPass 模式

手动 bypass

防火墙支持手动切换至 ByPass 模式，ByPass 模式下当前实例下所有流量均不会过防火墙，所有防火墙配置将失效，**建议在调试时使用**。
在防火墙实例页面，单击**更多 > 开启 ByPass / 关闭 ByPass**。

> **注意：**
> 调试完成请手动关闭 ByPass 模式。

自动 bypass

1. 在 VPC 间开关页面，单击**防火墙设置**。

2. 在防火墙设置页面，修改防火墙满载最长持续时间，当触发阈值后防火墙会自动 bypass。

> **注意：**
> 使用前请先升级引擎版本至最新。私有网络模式自定义路由引流暂不支持自动 bypass；云联网模式自定义路由引流自动启用 bypass 需优先配置好备用路由，详情请参见 查看/编辑备用路由 。

查看/编辑备用路由

备用路由是指当防火墙启用 bypass 模式后，VPC 将会自动切换至绑定的备用路由，您可以在控制台查看备用路由的绑定关系。

1. 在 VPC 间开关页面，单击**防火墙实例**，选择想要查看的防火墙实例，单击**实例详情**。

> **说明：**
> 当前版本仅云联网模式支持展示备用路由。

2. 单击**备用路由**，您可以在下方看到所有接入的 VPC 列表和其绑定的备用路由关系。
3. 单击**编辑**可以对 VPC 绑定的备用路由进行编辑，您可以选择一张路由表或选择未接入防火墙，选择未接入防火墙 bypass 时将不会操作此 VPC。

> **注意：**
> 编辑操作仅限自定义路由引流模式支持。

防火墙实例
规格调整
实例ID
云联网模式
实例名称
部署地域
北京
接入网络实例
关联防火墙
路由模式
防火墙网关地址
引擎版本
实例规格
1024 Mbps
总带宽规格：3272 Mbps
20000 条
已下发规则：280 条
接入网络实例
带宽限速
备用路由
同步路由
请输入搜索内容
ID/名称
下一跳类型
下一跳
操作
云联网
未接入防火墙
编辑

管理防火墙开关（主备模式）

最近更新时间：2024-08-19 09:42:41

在 防火墙开关页面，可通过开启或者关闭 VPC 间防火墙的开关，来实现对 VPC 间流量的管控。同时云防火墙会自动同步资产，因此不用担心资产变更后防火墙配置的问题，云防火墙在短时间内会自动同步。

> ⚠ **注意：**
> 开启/关闭防火墙操作涉及网络和路由切换，将会产生短时间网络抖动和闪断，请合理选择操作时间。

防火墙开关类型介绍

防火墙开关有4种类型：单点模式、多点模式、全互通模式、自定义路由。

- 单点模式：1个防火墙开关对应1对互通 VPC，1对互通 VPC 对应一个对等连接（或云联网）实例。
- 多点模式：1个防火墙开关对应1个 VPC，所有进出此 VPC 的流量均由此开关管理；一对 VPC 的互访会受两个开关分别独立控制。
- 全互通模式：1个防火墙开关对应1个防火墙的全部互通路由，开启开关防火墙即会接管全部接入的 VPC 流量。
- 自定义：由开关无实际意义，仅用于展示接入 VPC。

若变更对等连接（或云联网）实例，防火墙开关会对应同步变更，为了不影响您的业务，我们只会对状态为关闭的开关立即执行变更，请确保您在变更 VPC 间的对等连接（或云联网）的配置时，防火墙开关是关闭的。

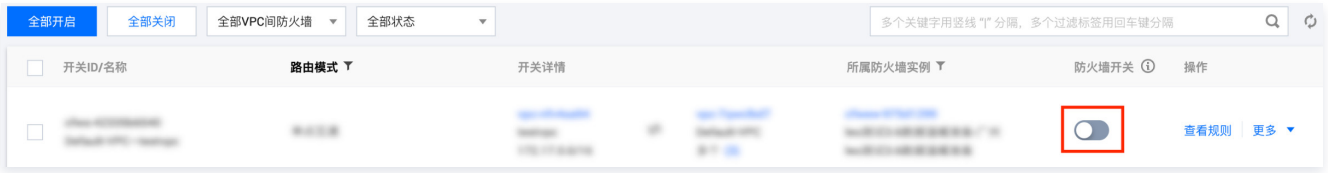
> ⚠ **注意：**
> 云防火墙不会打通基础网络，防火墙开关会根据可达路由自动生成，若无开关请检查是否存在对等连接或云联网。

开启开关

开启开关后，系统会自动修改相关路由表的路由策略，将所有防火墙开关对应的本端和对端网络间的流量牵引至 VPC 间防火墙。

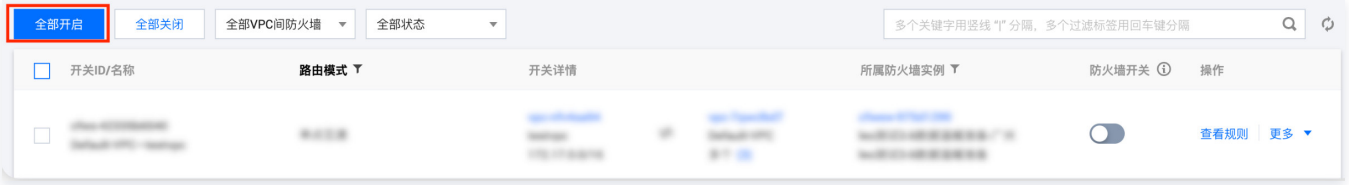
1. 在 VPC 间开关页面，单击**防火墙开关**，支持单个、批量、全部开启防火墙。

- 单个：选择所需防火墙，单击防火墙开关的，弹出确认开启弹窗。



- 批量： 勾选防火墙开关后，单击左上角的**批量开启**，弹出确认开启弹窗。

- 全部：未勾选任何项目时，单击左上角的**全部开启**，弹出确认开启弹窗。



2. 在确认开启弹窗中，单击**确定**，即可开启防护。

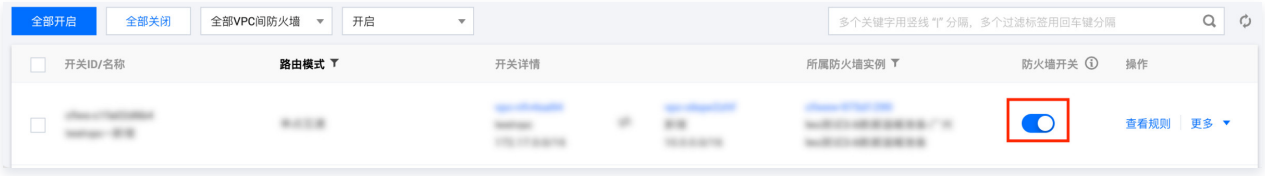
> ⚠ **注意：**

- 若 VPC 间没有正确配置对等连接（云联网）路由，防火墙无法开启。
- 开启后，请勿在“私有网络”（云联网）控制台中手动变更开关对应的路由，否则将导致防火墙丢失路由而引发网络中断。

关闭开关

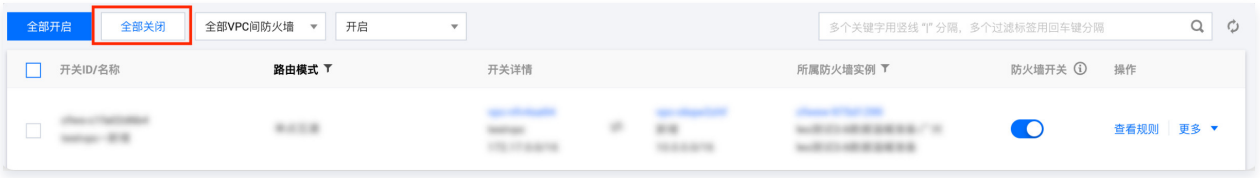
关闭开关后，系统会自动恢复相关路由表的路由策略，所有防火墙对应的本端-对端网络间的流量将恢复原先路径，不会经过 VPC 间防火墙。

1. 在 VPC 间开关页面，单击**防火墙开关**，支持单个、批量、全部关闭防火墙。
   - 单个：选择所需防火墙，单击防火墙开关的，弹出确认关闭弹窗。



   - 批量：勾选防火墙开关后，单击左上角的**批量关闭**，弹出确认关闭弹窗。

   - 全部：未勾选任何项目时，单击左上角的**全部关闭**，弹出确认关闭弹窗。

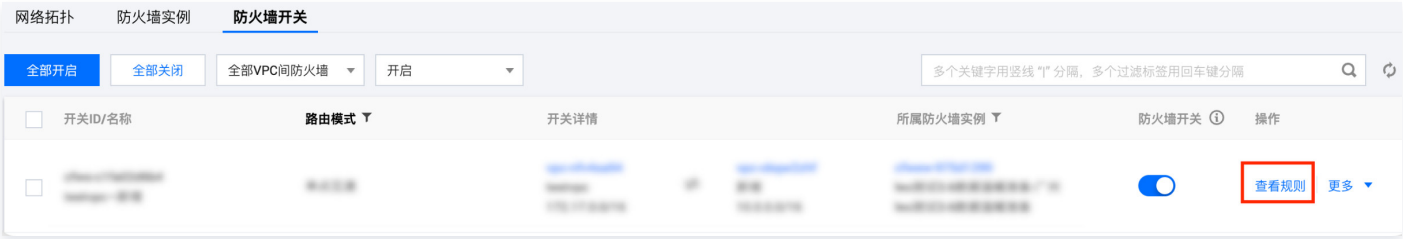


2. 在确认关闭弹窗中，单击**确定**，即可关闭防护。

> **注意：**
> 关闭后，您可以根据需要切换 VPC 路由，但切勿手动启用防火墙路由，否则将导致网络中断，防火墙开关故障。

查看规则

1. 在 VPC 间开关页面，单击**防火墙开关**。
2. 在防火墙开关页面，选择所需防火墙开关，单击**查看规则**。



3. 在内网间规则页面，可以对规则进行查看和编辑，操作详情请参见 访问控制-内网间规则 。

查看日志

1. 在 VPC 间开关页面，单击**防火墙开关**。
2. 在防火墙开关页面，单击**更多** > **查看日志**，可以选择查看流量访问控制日志或流量日志。

使用网络拓扑（主备模式）

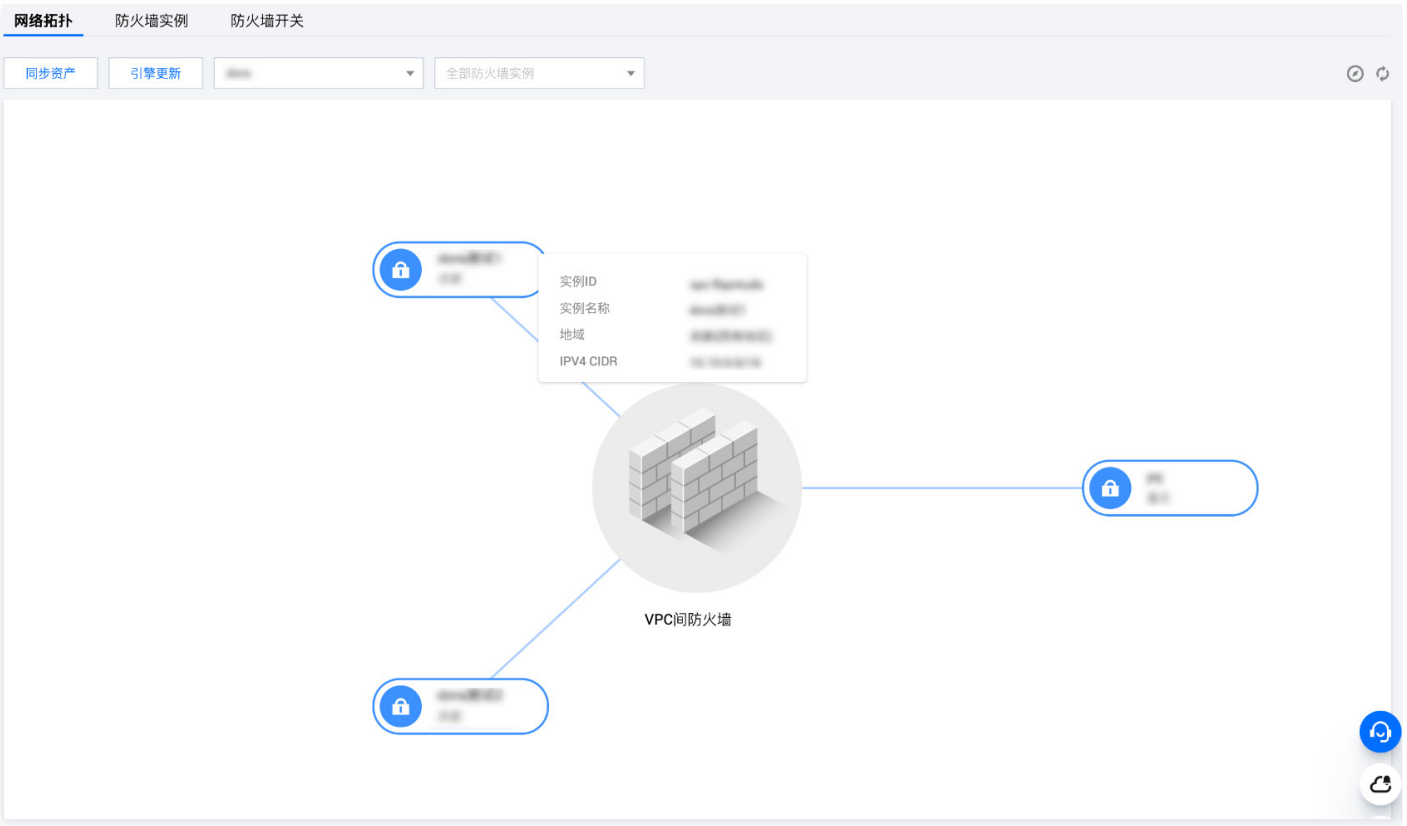
最近更新时间：2024-10-17 20:59:31

查看网络拓扑

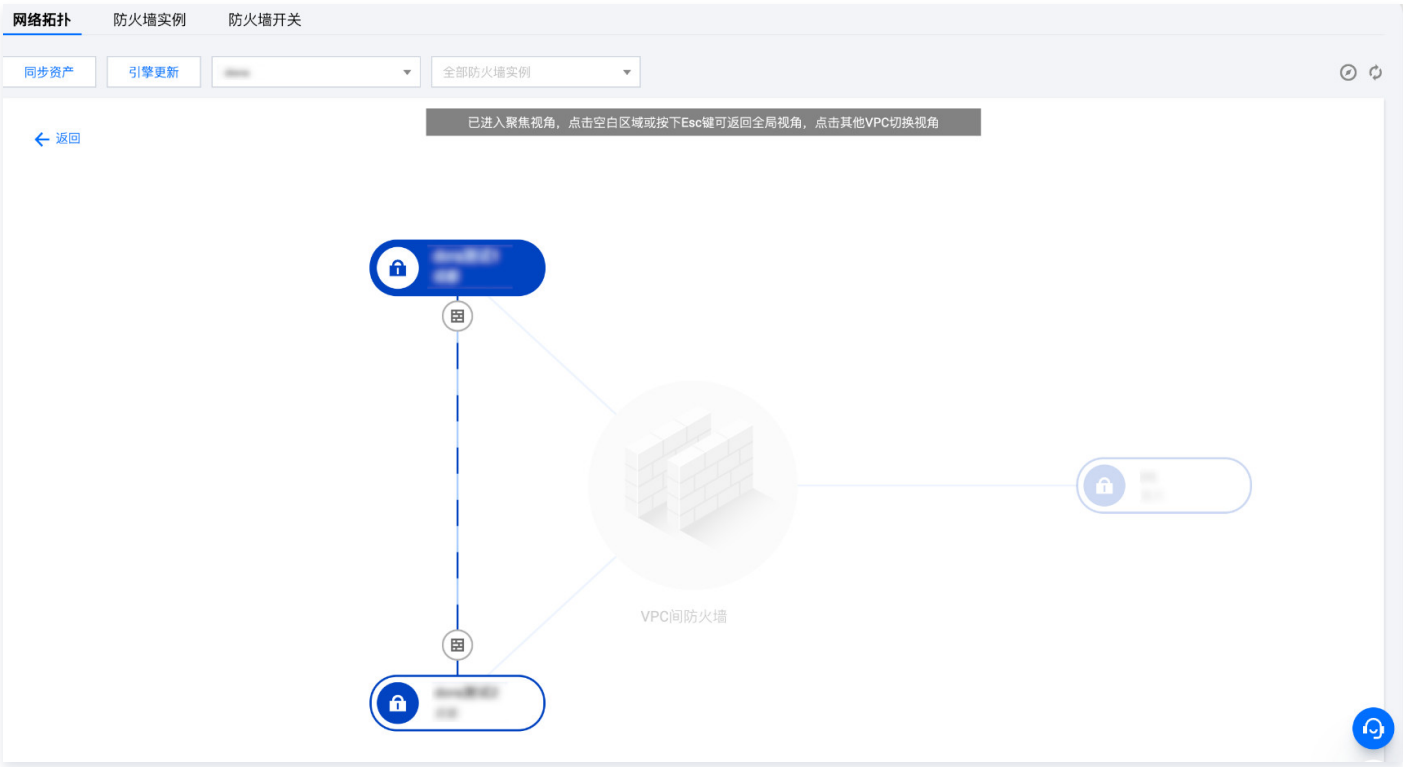
云防火墙提供了一个可视化视图，帮助您快速梳理 VPC 间资产的访问关系。

> **说明：**
> 自定义路由方案下暂无网络拓扑图

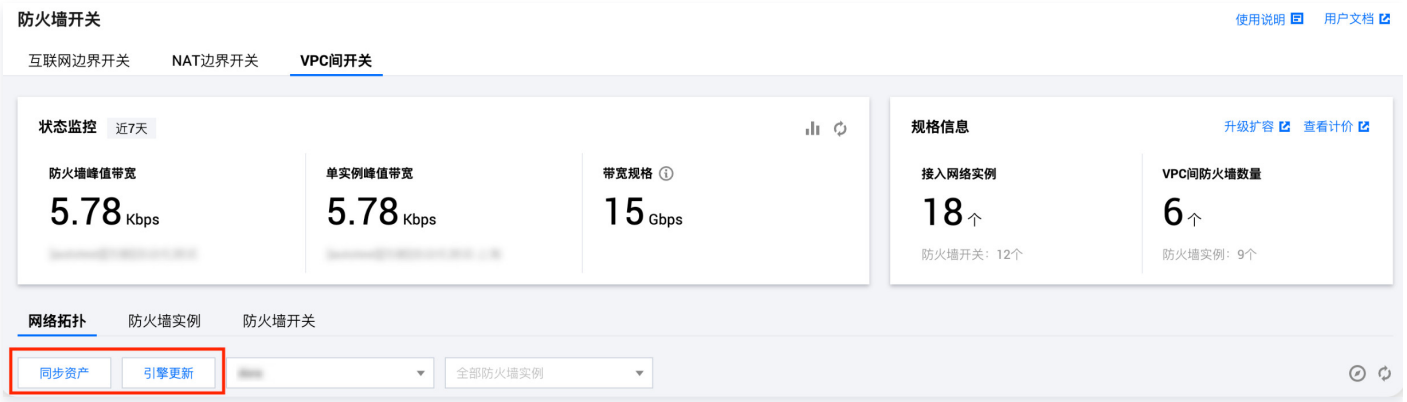
1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **VPC 间开关**。
2. 在VPC 间开关页面，单击**网络拓扑**，查看接入的 VPC 网络实例详情。
3. 在网络拓扑页面，鼠标悬停在某个 VPC 实例，可以查看该实例的详细信息。



4. 单击**某个实例**，可查看与其他 VPC 实例的连接情况，以及防火墙开关开启情况。防火墙开关标识如果**深蓝色则代表开关开启，如果是灰色则代表开关关闭**。



5. 在网络拓扑页面，单击**同步资产**，可以及时同步资产信息；将鼠标悬停引擎更新处可以查看版本信息。

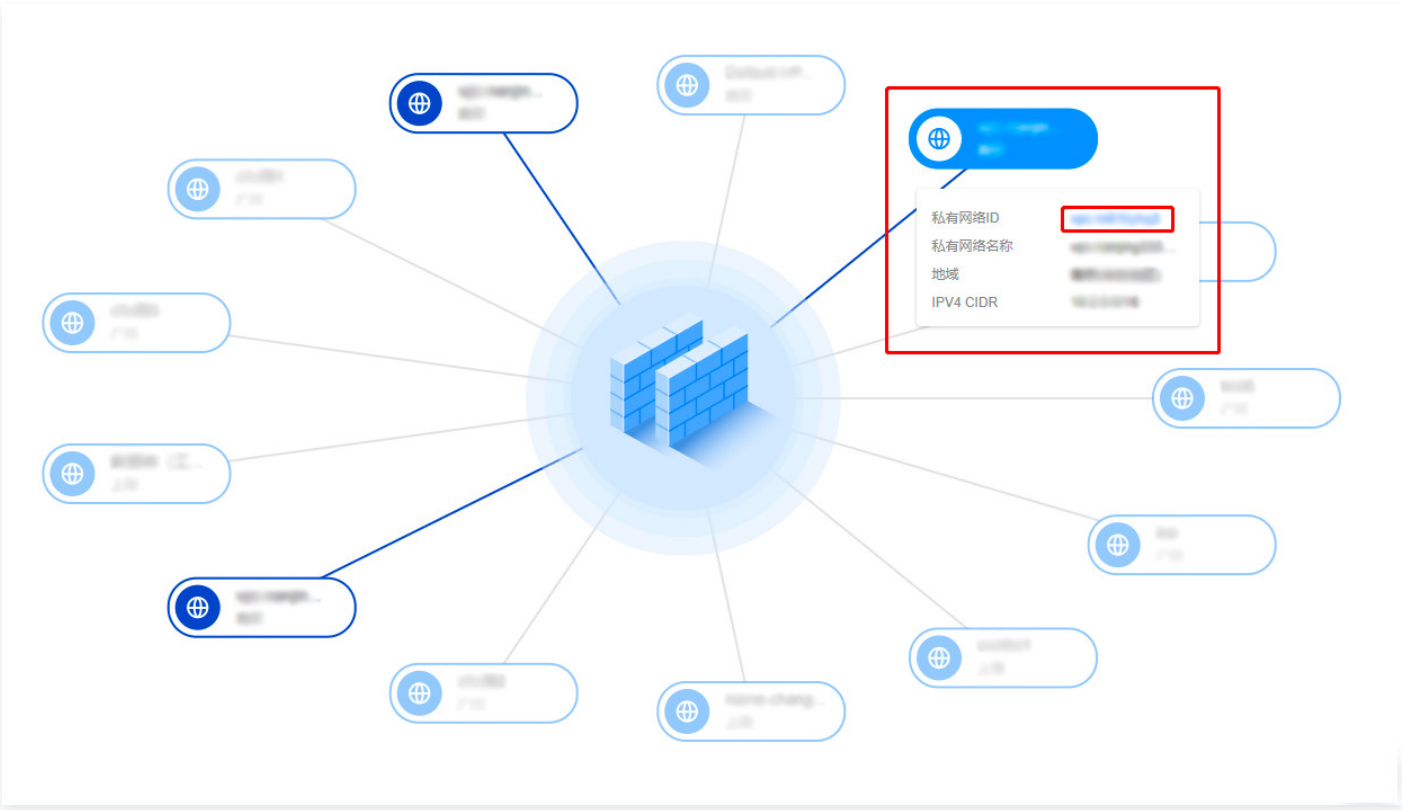


6. 在网络拓扑页面，单击右上角的或，可查看操作指引或刷新网络拓扑。

使用 VPC 视图梳理 VPC 间的访问关系

云防火墙提供了一个可视化视图，帮助您快速梳理 VPC 之间的访问关系。在 VPC 可视化视图中，每个节点是一个 VPC 实例，VPC 间防火墙是一个中心化的设备，每个开关控制了不同的路由。已开启开关的 VPC 间流量将会被牵引至防火墙进行过滤与防护。

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关 > VPC 间开关**。
2. 在VPC 间开关页面，单击**网络拓扑**，查看接入的 VPC 网络实例详情。
3. 将鼠标在某个 VPC 节点上悬停，可查看 VPC 的简要信息，同时与之互联的所有 VPC 也会亮起。单击私有网络 ID 的**蓝色字体**，可进入 VPC 详情页查看该 VPC 的详细信息。



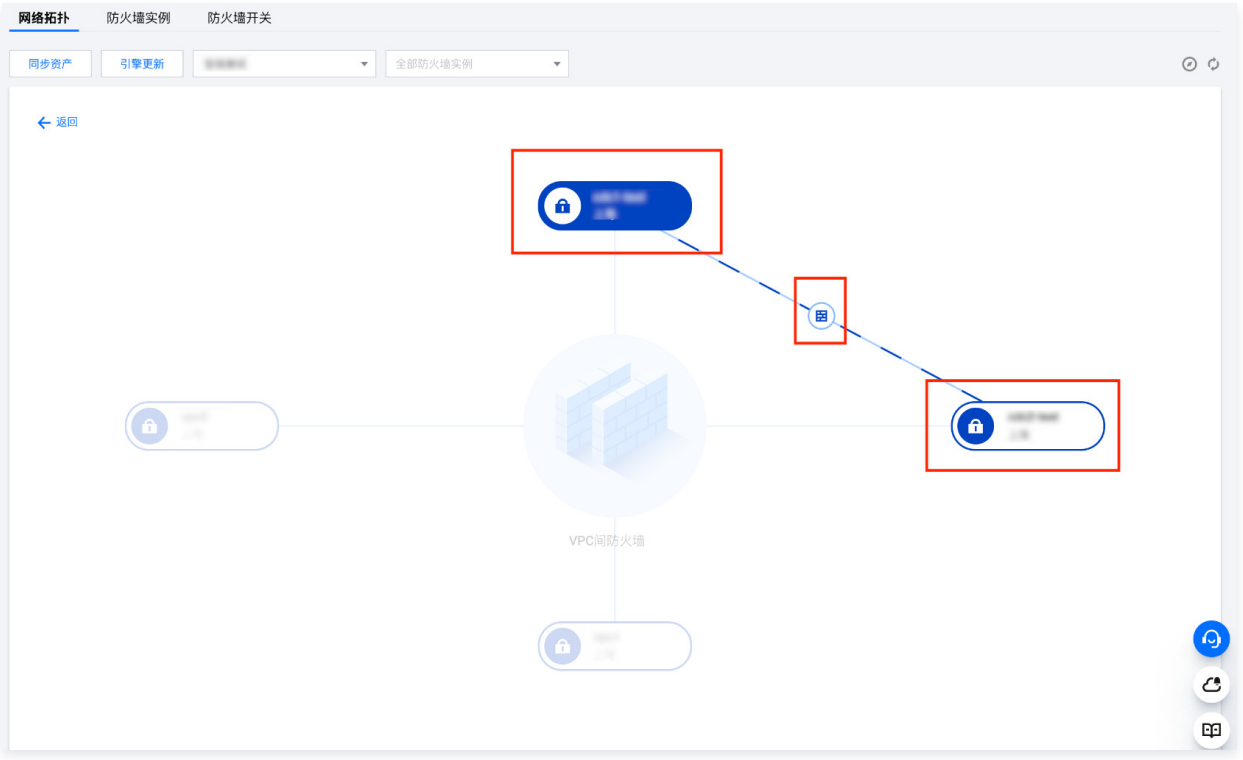
4. 可以单击**某个 VPC 节点**，页面进入聚焦视图，显示以聚焦 VPC 为中心的拓扑结构。
5. 彼此互通的 VPC 间通过连线相连接，连线中可以查看或操作防火墙开关，也可以通过单击防火墙的，直接进入访问控制规则配置页面。

注意

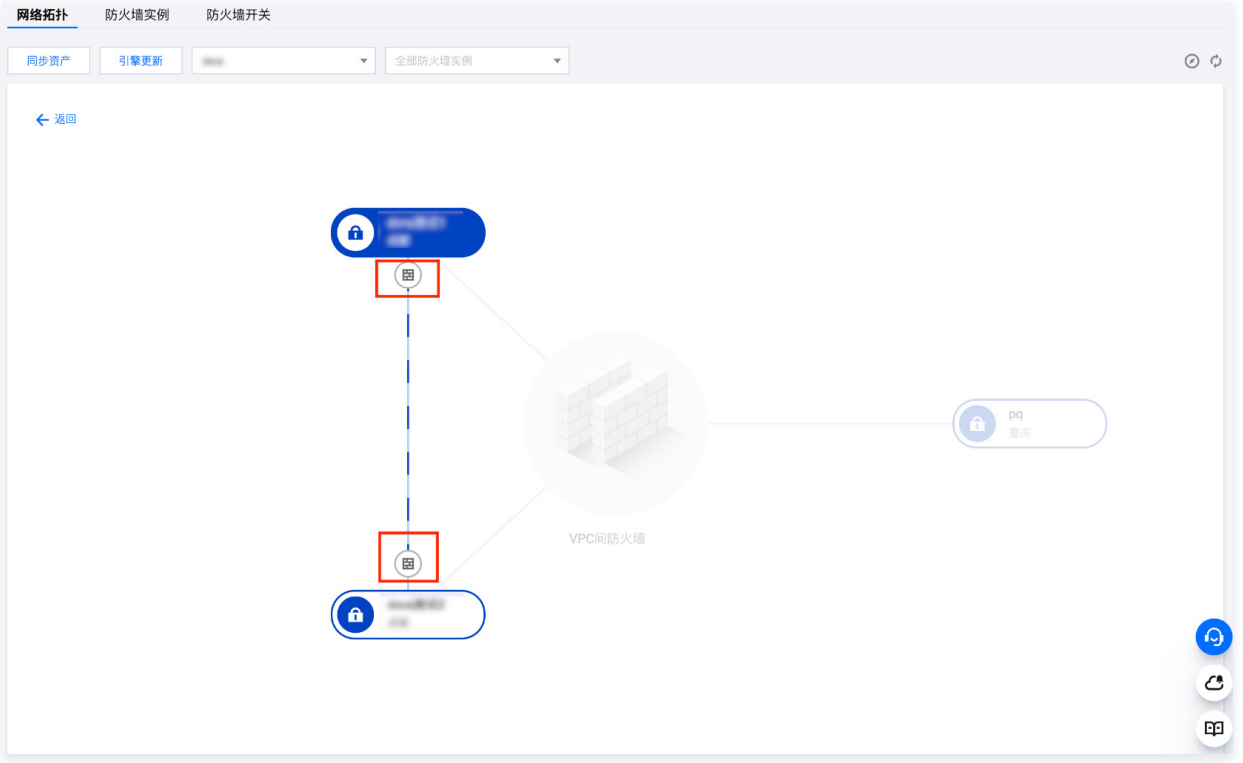
- 单点互通模式下每对可互相访问的 VPC 在图上仅会展示1个开关。
- 多点互通模式下每个 VPC 会展示1个开关。

- 全互通模式 VPC 间防火墙仅会有1个开关。

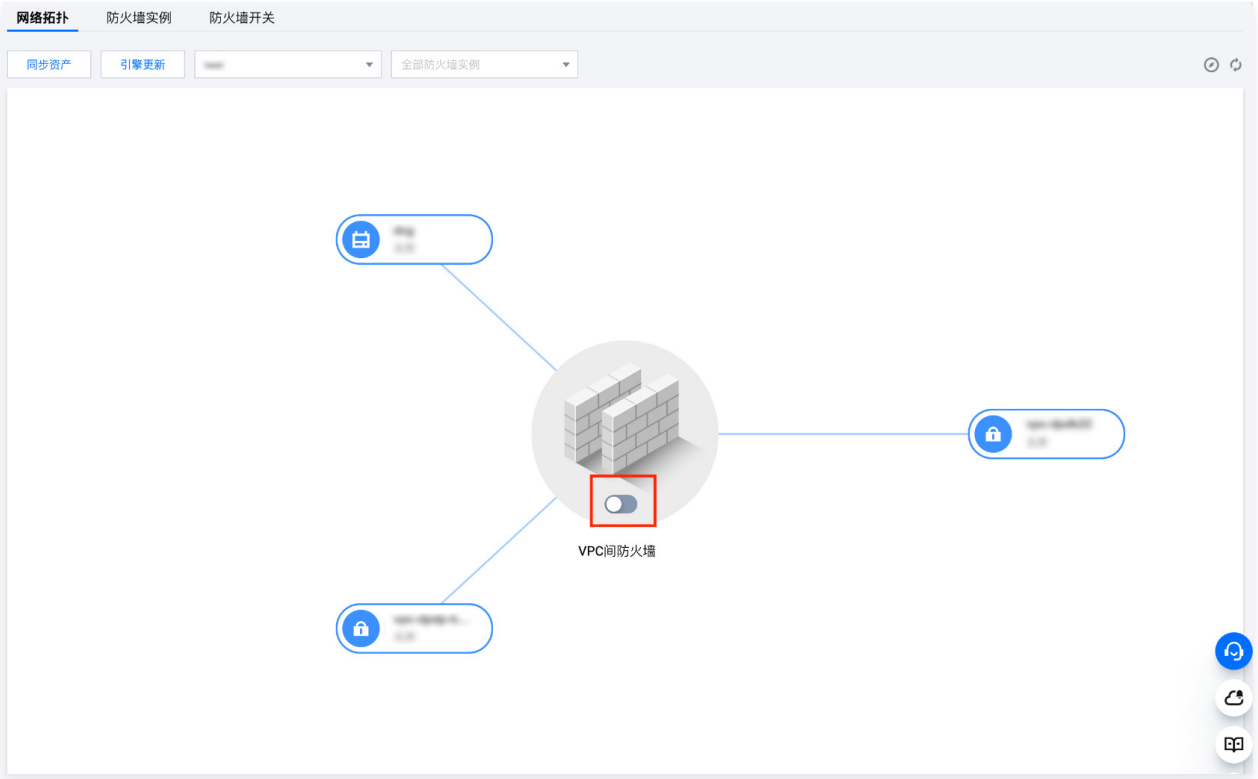
○ 单点互通模式



○ 多点互通模式



○ 全互通模式



自定义路由配置指引（主备模式）

概述

最近更新时间：2024-04-22 17:25:32

VPC 间防火墙自定义路由模式下，用户可以对路由进行自定义配置，实现个性化引流和防护的方案。

> **注意：**
> 在使用自定义路由模式前，请确认基础网络已经打通（可通过对等连接或云联网），云防火墙无法进行基础的网络打通。

基本概念

防火墙实例

用于承载防火墙功能的虚拟化实例，与 CVM 类似，可前往 云防火墙控制台 查看。

防火墙引流 VPC（云联网模式）

由防火墙在云联网创建的专用 VPC，用于将用户网络流量通过防火墙引流 VPC 牵引至防火墙实例，从而实现防护效果，请勿删改。一般命名为“防火墙专用 VPC_请勿删改”。可以前往 云联网实例详情控制台 查看。

> **说明：**
> 防火墙会在每个地域分别创建不同的 VPC 用于对应地域流量的引流。

防火墙路由表（云联网模式）

防火墙自动创建的路由表，用于分配流量，请勿手动修改。一般命名为“防火墙 VPC 专用路由表_请勿删改”。

> **注意：**
> 每个地域会创建一张用于防火墙的路由表。

防火墙引流 VPC

由防火墙在云联网创建的专用 VPC，用于将用户网络流量通过防火墙引流 VPC 牵引至防火墙实例，从而实现防护效果，请勿删改。一般命名为“防火墙专用 VPC_请勿删改”。可以前往 云联网实例详情控制台 查看。

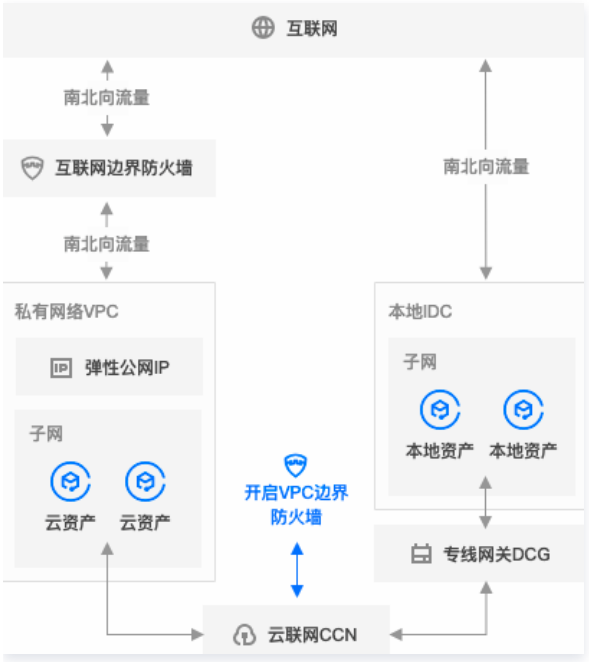
> **说明：**
> 防火墙会在每个地域分别创建不同的 VPC 用于对应地域流量的引流。

工作模式

私有网络模式

云联网模式

VPC 间防火墙和所有业务 VPC 在同一个云联网中，通过建立一个防火墙专用 VPC 网段来将用户 VPC 互访的流量牵引至防火墙。



私有网络模式

最近更新时间：2024-10-17 21:08:21

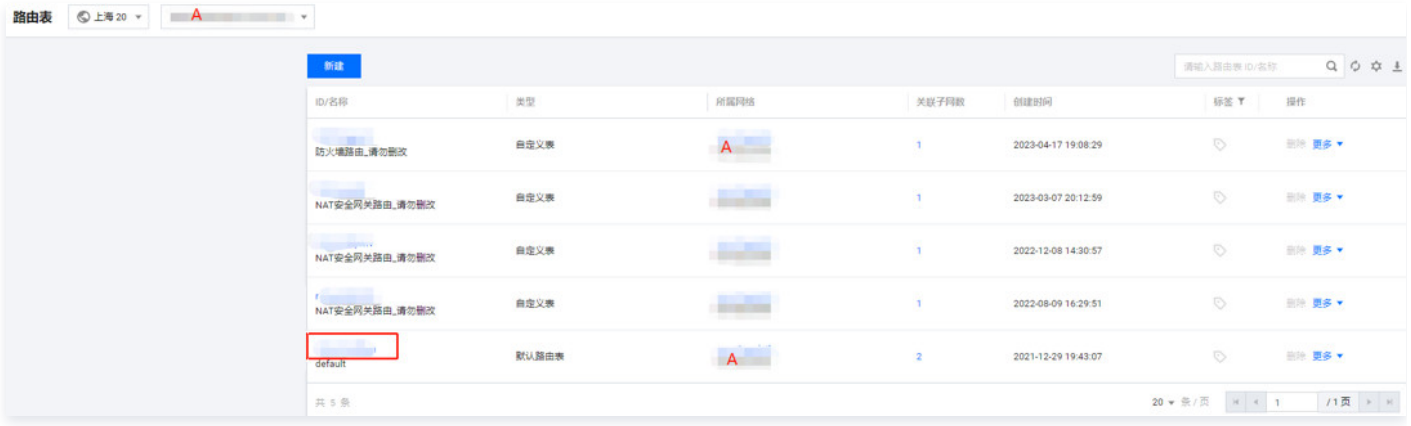
步骤1：创建自定义路由模式实例

参考 VPC 间防火墙开关-新建 VPC间防火墙，创建目标实例，其中路由模式选择**自定义路由**。

步骤2：配置引流路由

查看对等连接两端 VPC，分别为 VPC A 与 VPC B。

1. 在 路由表页面，查找 VPC A 的路由表，并单击该路由表的 ID。选择 **default 路由表**。



2. 在详情页面，单击**新增路由策略**。
3. 在新增路由弹窗中，添加目的端为 VPC B 网段，下一跳为高可用虚拟 IP 的路由策略，单击**创建**。

4. 在详情页面，关闭原本对等连接的路由开关，并立即启用刚刚配置的路由。

> **注意：**
> 切换路由网络会出现闪断，建议在业务低峰期操作。

5. 在路由表页面，查找 VPC B 的路由表，选择 default 路由表。

6. 重复之前的动作，添加防火墙路由条目。

步骤3：验证防火墙是否正常工作

1. 参考 日志审计 查看是否有流量日志。
2. 参考 日志审计 查看入侵防御是否正常。
3. 配置内网间规则，检查是否正常命中。

至此防火墙已正常工作，如果您的网络结构较为复杂或涉及专线场景，请 提交工单 咨询详细路由配置方案；如果您有更多疑问也欢迎 提交工单 联系我们。

云联网模式

最近更新时间：2024-04-22 17:25:32

步骤1：创建自定义路由模式实例

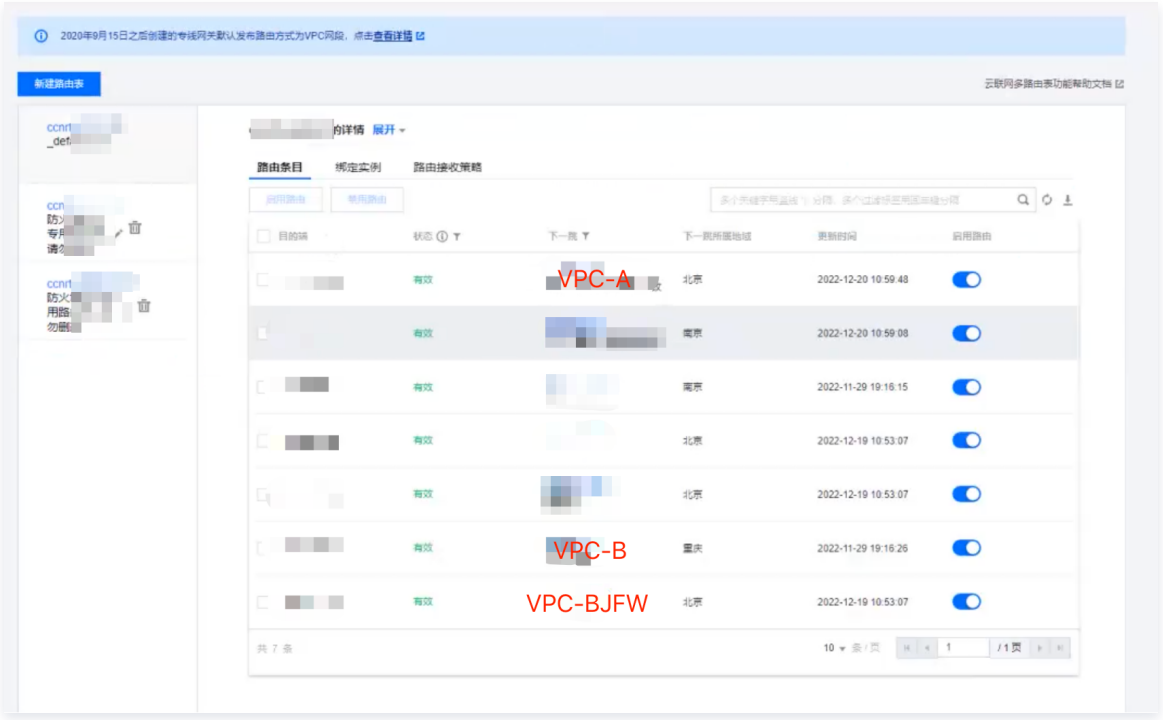
参考 新建 VPC 间防火墙，创建目标实例，其中模式选择**自定义路由**。

步骤2：配置引流路由

当前操作目的是将用户需要防护的业务 VPC 通过防火墙网关引流至防火墙实例。

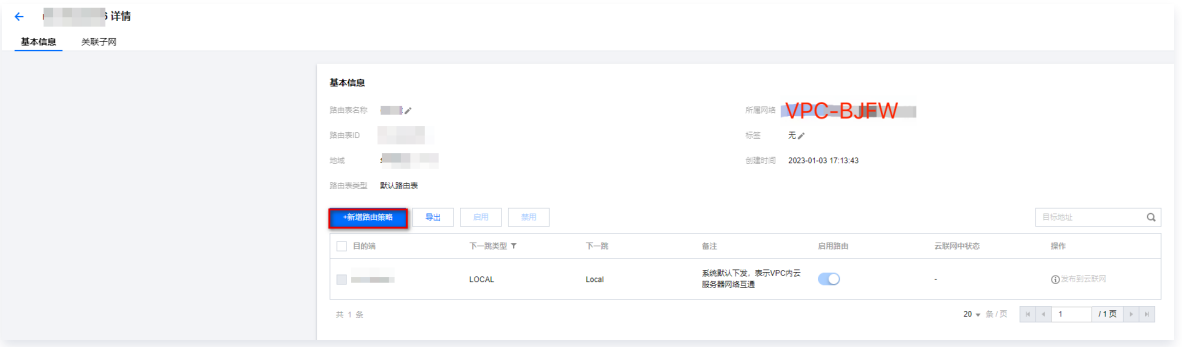
1. 前往 新建 VPC 间防火墙 时选择的云联网实例的控制台，查看高级模式关联的云联网实例详情。
2. 确认防火墙引流 VPC 和相关路由表已经创建，若未创建请等待实例创建完成或 提交工单 联系我们。
3. 查看默认路由表页面，确定需要接入的业务 VPC 及防火墙引流 VPC。

> **说明：**
> 本文以北京业务 VPC：VPC-A；重庆业务 VPC：VPC-B；北京地域防火墙引流 VPC：VPC-BJFW 举例来演示如何接入。



4. 前往**私有网络** > 路由表 页面，选择需要接入的防火墙引流 VPC，可以看到包含“防火墙 VPC 专用路由表_请勿删改”和“default”在内的路由表。选择“default”路由表编辑路由策略。

5. 单击**新增路由策略**，将业务 VPC 下一跳引流至防火墙。



目的端输入业务 VPC 的 CIDR，下一跳类型选择**高可用虚拟 IP**，下一跳选择**防火墙网关 ID**，备注可以自由填写。

> **说明：**
> 若有提示“指定 CIDR 形成 ECMP”时，需要先在默认路由表中停用相关业务路由。

6. 将新增路由发布到云联网，详情请参见 管理路由策略 。发布后可以在对应云联网中的默认路由表看到指定路由策略。

> **说明：**
> 因新路由策略与原路由策略冲突，原路由条目会失效，可以忽略。

步骤3：建立业务 VPC 互访路由表

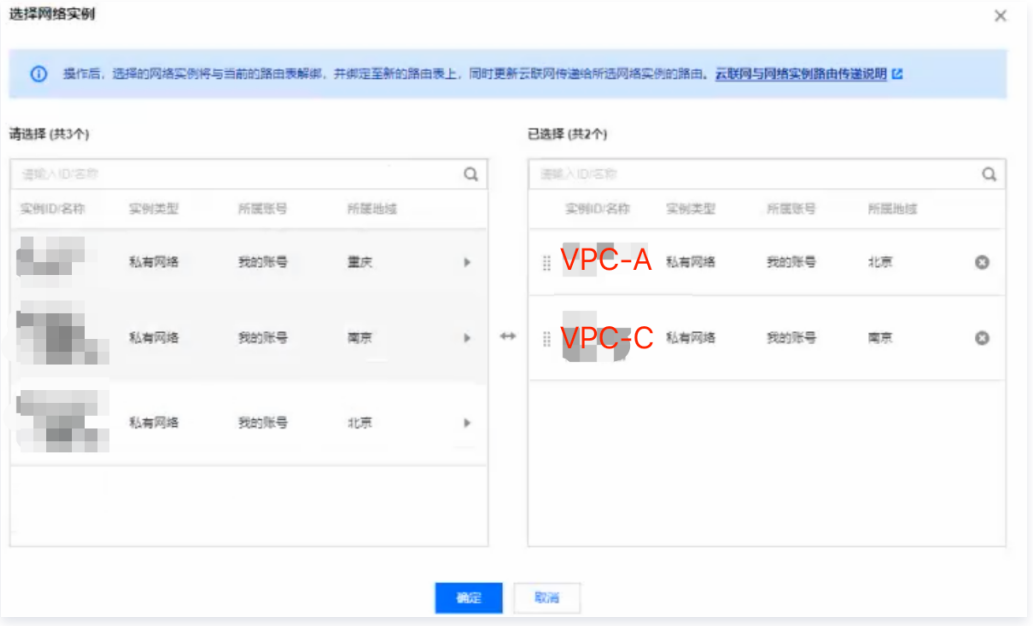
当前操作目的是为了将防火墙网络和用户的业务网络打通，实现网络互访。

1. 在 云联网页面，分别为每个引流至防火墙的业务 VPC 建立路由表。

2. 调整路由接收策略。在各个 VPC 的专属路由表中的**路由接收策略**中单击**添加网络实例**，将路由表自身所属 VPC 实例和互通 VPC 实例添加至路由表中。

> **注意：**
> 添加网络实例务必分为两个步骤，先添加自身 VPC 实例和不经过防火墙防护的 VPC 实例；再添加防火墙引流专用 VPC 实例。

例如：假设 VPC-C 是不需要接入防火墙实例的业务 VPC，则在 VPC-A 的路由表中应先添加 VPC-A，VPC-C 两个实例，添加成功后，重复上述操作再添加 VPC-BJFW 一个实例。



3. 检查各个 VPC 的专属路由表中路由条目是否符合预期。
4. 绑定网络实例。各个 VPC 的专属路由表的**绑定实例**单击**绑定网络实例**，将各个 VPC 专属路由表绑定至其对应的 VPC 实例，操作完成后网络会引流至防火墙。

> **注意：**
> 请务必确认路由无误后再绑定路由表，绑定后会立即生效。

步骤4：验证防火墙是否正常工作

1. 参考 日志审计 查看是否有流量日志。
2. 参考 日志审计 查看入侵防御是否正常。

> **注意：**

> 自定义路由模式下的入侵防御模式跟随主模式，无法单独调节。

3. 配置内网间规则，检查是否正常命中。

至此防火墙已正常工作，如果您的网络结构较为复杂或涉及专线场景，请 提交工单 咨询详细路由配置方案；如果您有更多疑问也欢迎 提交工单 联系我们。

资产中心
概述

最近更新时间：2025-07-01 16:12:12

资产中心统计了用户资产的相关数据及信息，通过资产分组、资产分类等方便用户检索资产信息，帮助用户更好地把控资产现状、管理资产并预知和防控安全事件。根据不同的分类逻辑，将资产中心划分为资产总览、按资产分组、按资产类型、按服务类型四个部分。

- 资产总览：包含了所有类型的资产个数统计、流量统计、攻击风险统计概况。
- 资产分组：支持用户自定义分组等方式，帮助用户组织和梳理现有资产，方便查看资产信息。
- 资产类型：通过将资产划分为主机、公网 IP、域名等类型，分类进行资产信息展示，以及资产暴露风险统计等。
- 服务类型：通过全流量检测与响应NDR自动识别网络资产，精准识别资产组件及服务类型，建立资产清单，助企业了解资产状况，避免遗漏与管理盲区。采用被动识别方式，对业务无侵入。

版权所有：腾讯云计算（北京）有限责任公司

资产总览

最近更新时间：2025-05-09 16:09:22

资产统计概况

通过资产统计概况，可以快速地了解当前用户资产个数，以及主要的暴露风险，把握资产现状、并预知和防控安全事件。

1. 登录 云防火墙控制台，在左侧导航中，单击**资产中心**。

2. 在资产中心页面，左侧为资产与风险个数统计概况，单击**资产数字**，可跳转到**对应的资产类型**页查看资产详情。
3. 用户可在页面右侧，选择查看近24小时、7天或30天内的资产信息，包括流量、带宽、资产使用率等TOP5 资产信息。

资产更新

后台定时轮询用户资产信息的间隔为10分钟，因此当用户资产规模在此间隔内发生变化，但尚未被后台同步时，在 资产中心 页面，单击**资产更新**，及时调用后台接口重新读取并同步用户的资产信息与数据。

资产分组

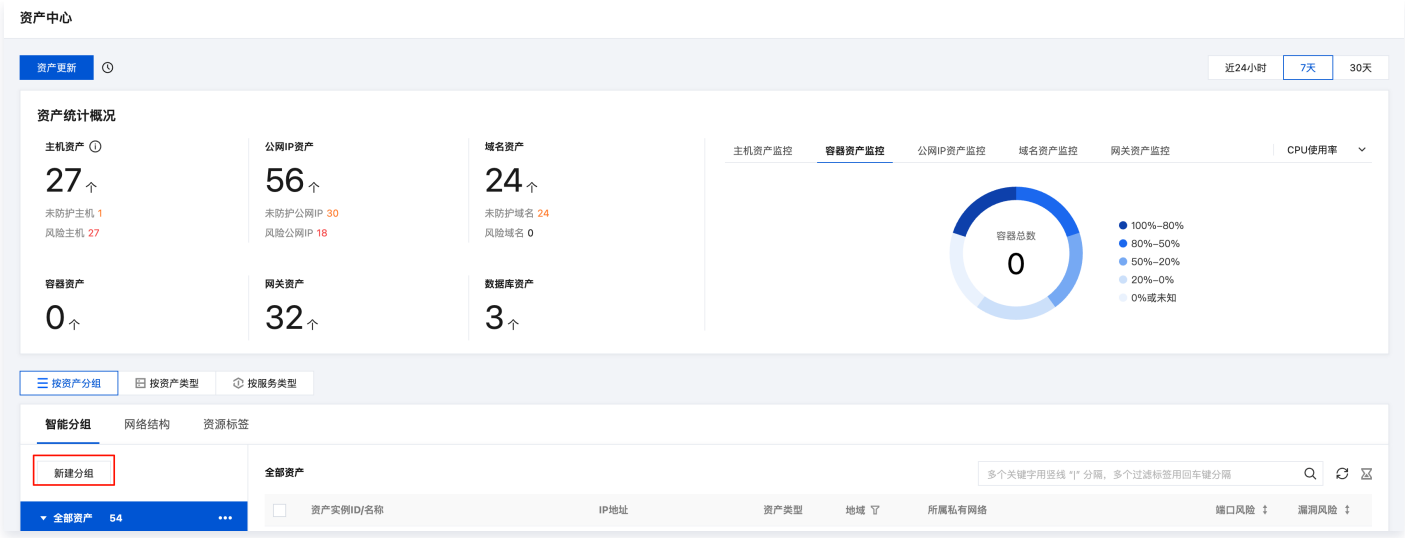
资产中心支持用户自定义分组的方式对资产进行梳理并分组查看，方便用户快速把握当前资产的组织信息。

> **注意：**
> 首次使用时，云防火墙会基于用户的资源标签生成默认分组信息，用户可以根据需要自行调整分组或重置分组。

新建分组

方法一

1. 在 资产中心 > **按资产分组** > **智能分组**页面，单击**新建分组**，创建新的资产分组。



2. 新建资产分组弹窗中，选择资产加入分组的方式：
   - 手动添加：从现有资产中手动选择加入分组的资产。选择新分组的父分组，以及填入分组名称，单击**确定**，完成新建分组。

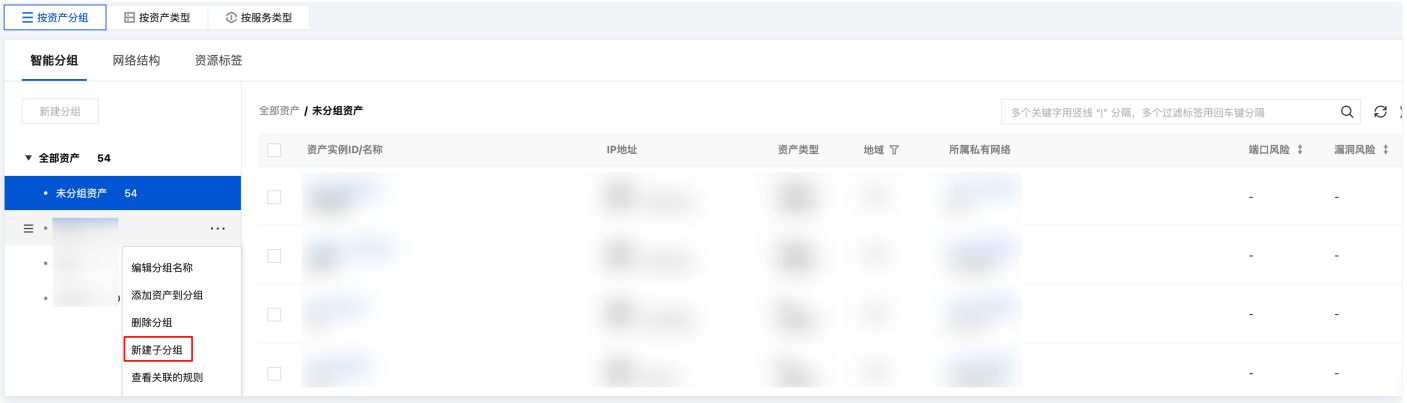
> **说明：**
> 父分组为已经创建过的分组，将新分组加入到父分组下的资产信息中，层层管理。

- 从参数模板导入：从现有的参数模板选择，将模板中全部 IP 地址识别为资产并自动加入到一个分组。

> **注意：**
> 创建分组后，参数模板的变化不会自动同步到分组。

方法二

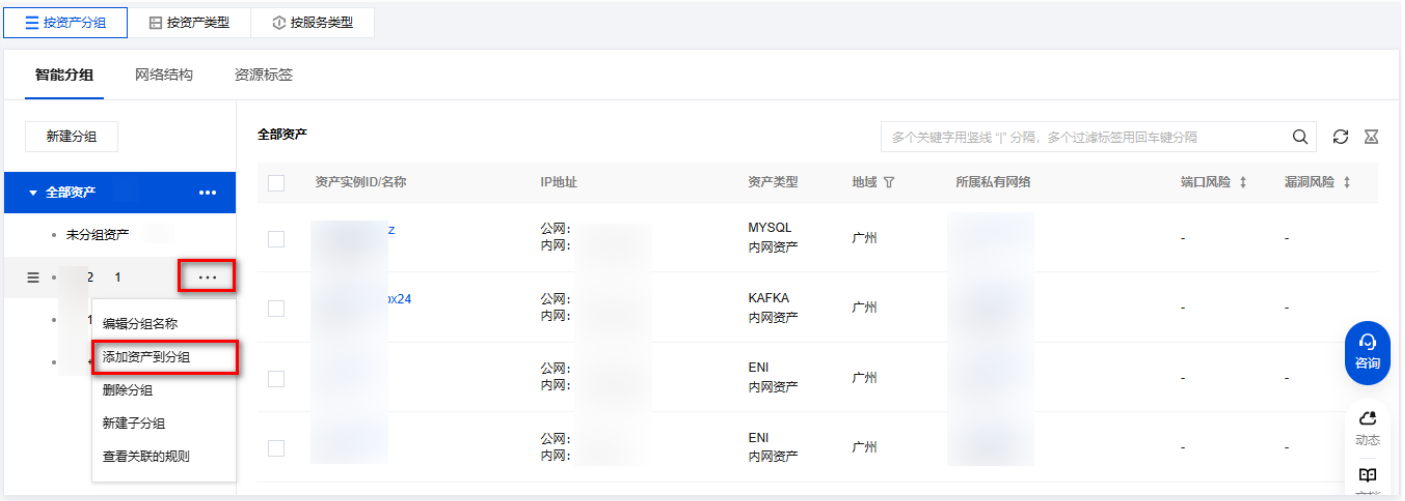
1. 在 资产中心 > **按资产分组** > **智能分组**页面，单击分组的...图标，在下拉框中选中**新建子分组**。



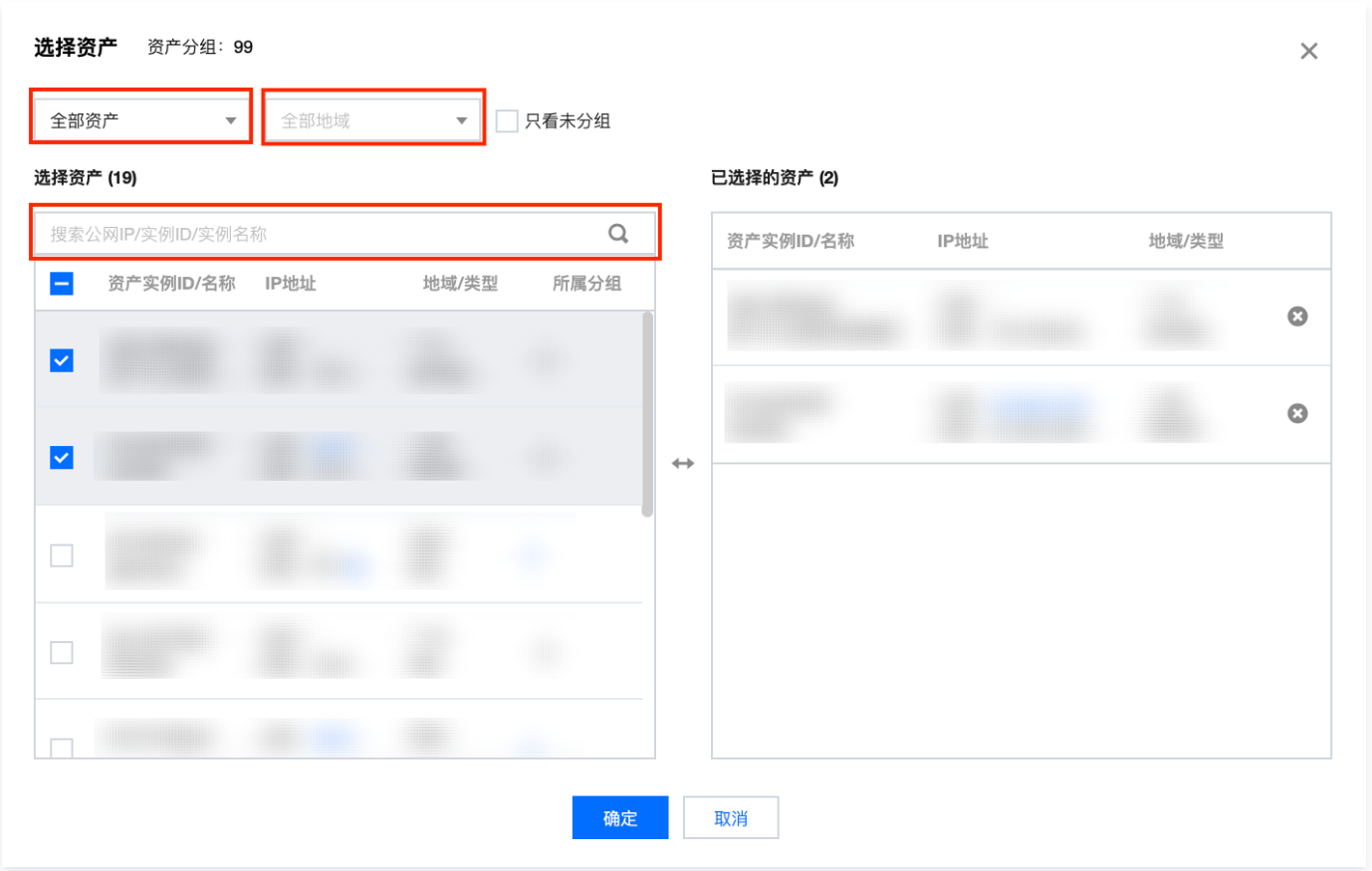
2. 在弹窗中填入子分组名称，单击**确定**，完成创建。

添加资产至新分组

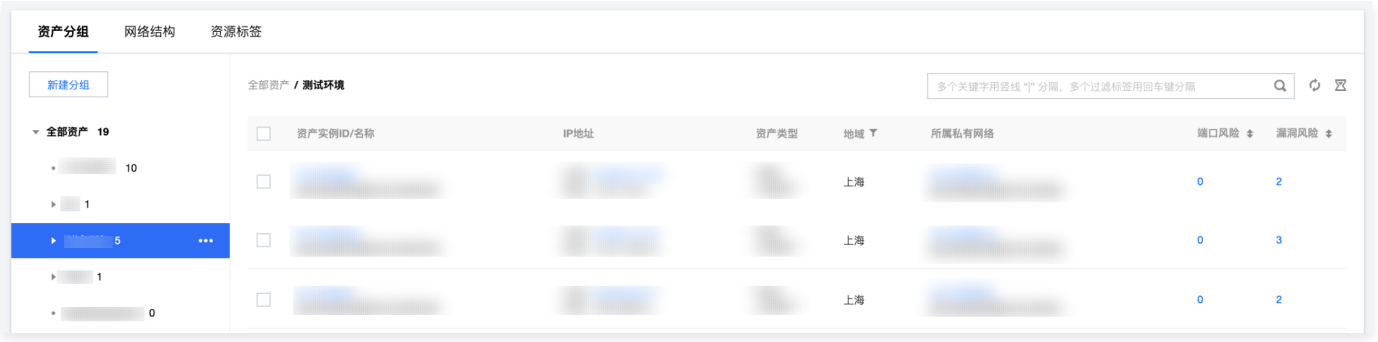
1. 在 资产中心 > **按资产分组** > **智能分组**页面，单击分组的...图标，在下拉框中选中**添加资产到分组**。



2. 在选择资产弹窗中，根据资产类型、所在地域、搜索公网 IP/实例 ID/实例名称，进行资产筛选，选择加入新分组的资产。

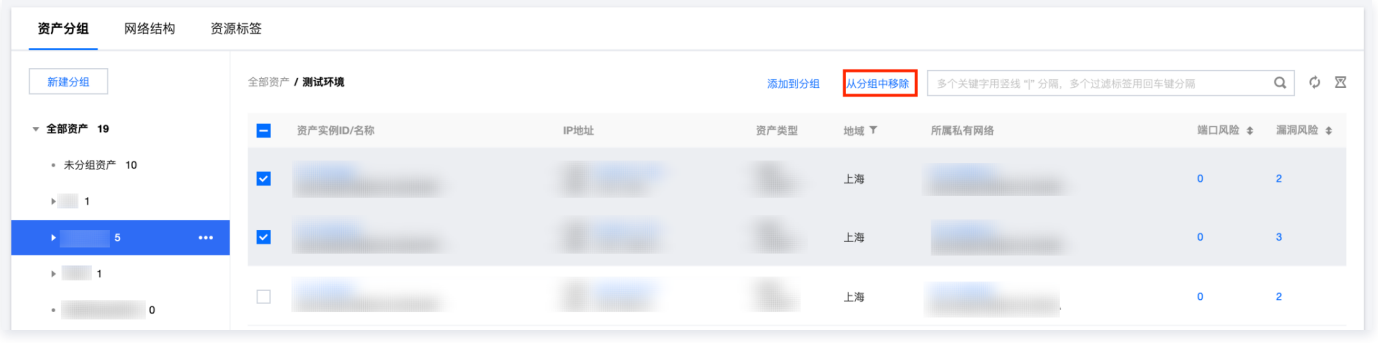


3. 添加资产完成后，在该分组的右侧资产列表中，出现已添加到此分组的资产列表。



在分组中移除资产

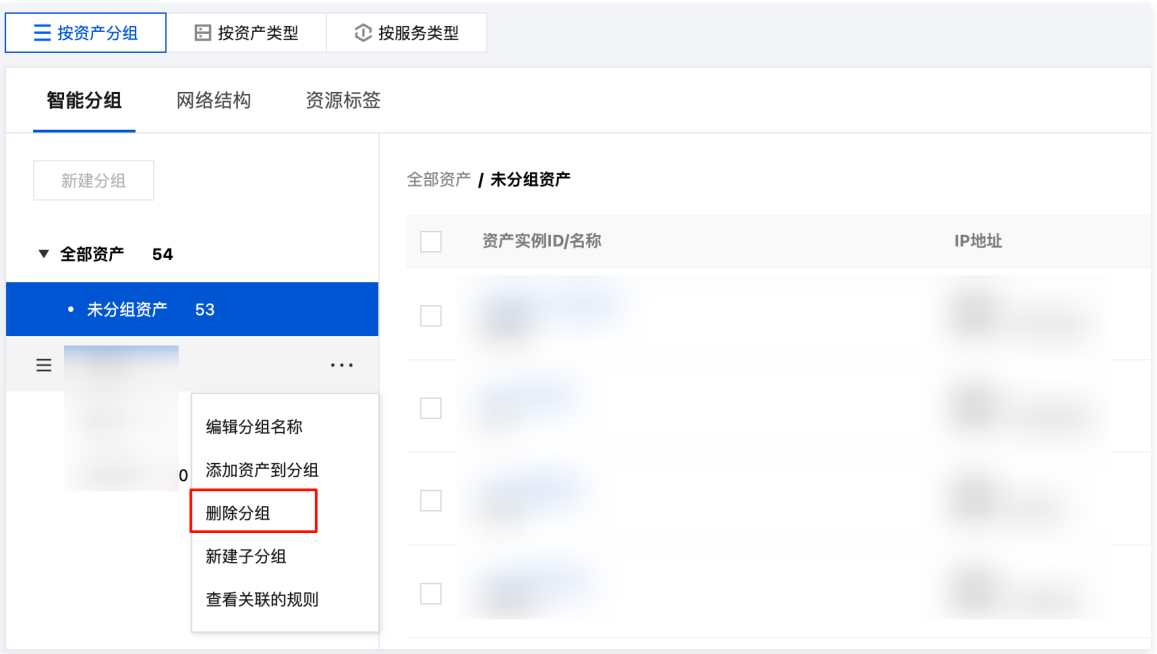
1. 在 资产中心 > **按资产分组** > **智能分组**页面，勾选指定资产，单击**从分组中移除**。



2. 在确认弹窗中，单击**确定**，完成移除。

删除分组

1. 在 资产中心 > **按资产分组** > **智能分组**页面，单击分组的...图标，**单击删除分组**。



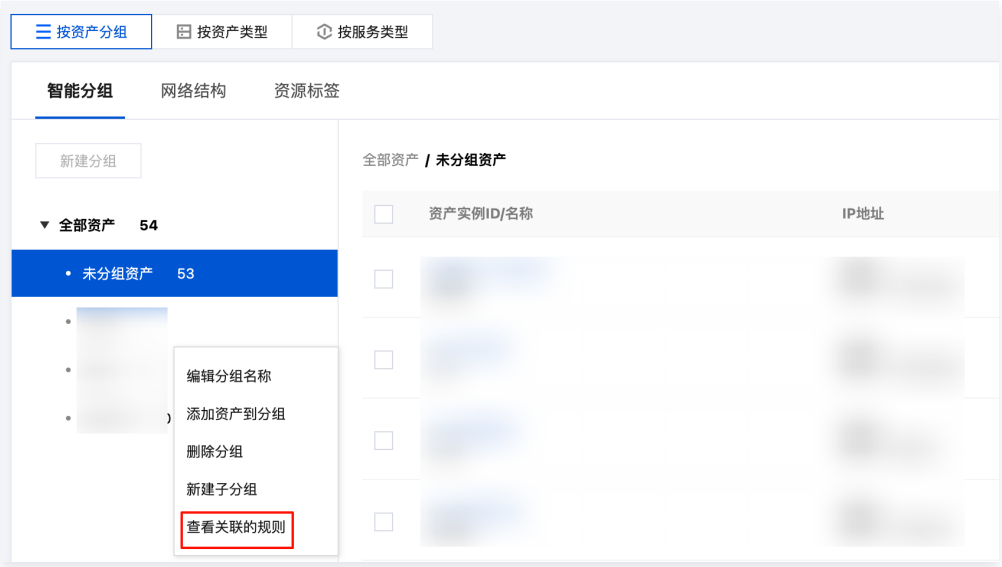
2. **在确认弹窗中，单击确定，删除资产分组。**

注意：

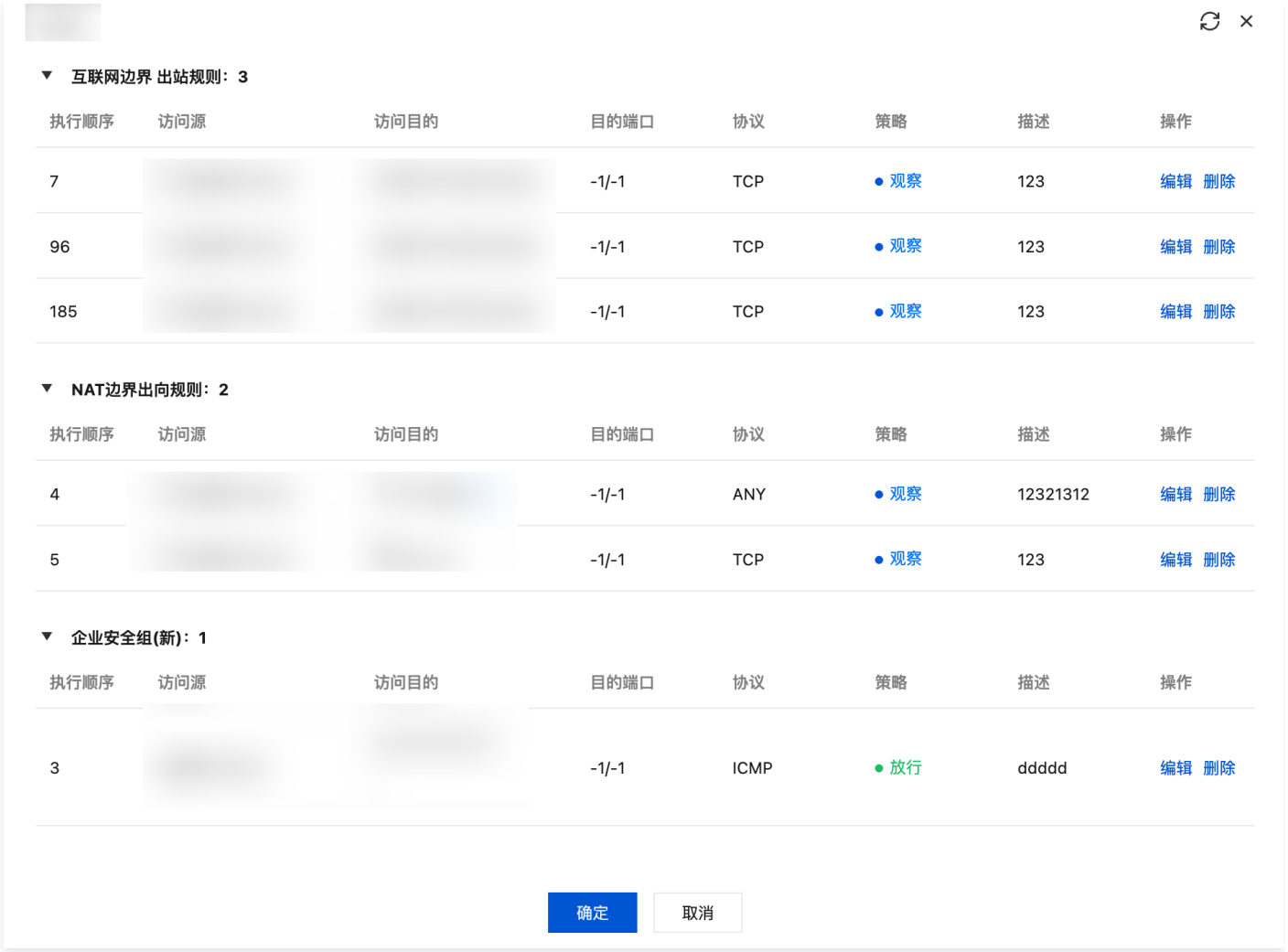
若当前资产分组有被用于安全策略的配置则不可删除，请手动删除所有规则后再尝试操作。

查看分组的关联规则

1. 在 资产中心 > **按资产分组** > **智能分组**页面，单击分组的...图标，单击**查看关联的规则**。



2. 在弹窗中，可查看该分组关联的规则列表，可直接在弹窗中进行规则编辑与删除操作。



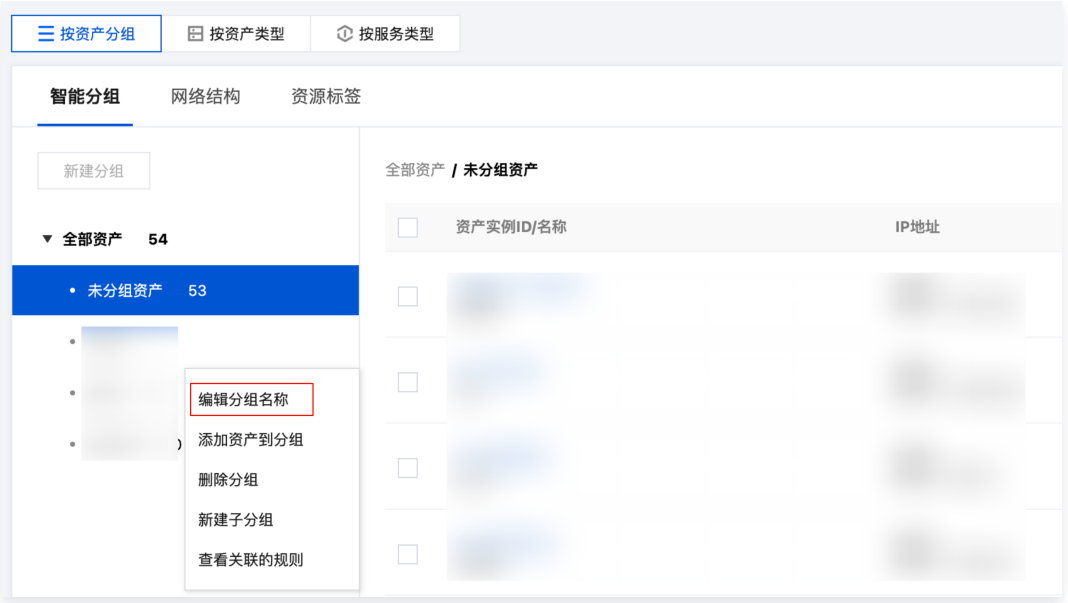
调整分组位置

方法1：通过手动拖拽的方式

1. 在 资产中心 > **按资产分组** > **智能分组**页面，选中想要调整位置的分组，单击左侧三，进入拖拽状态。
2. 将分组拖拽到想要调整的位置处释放即可。

方法2：编辑分组名称

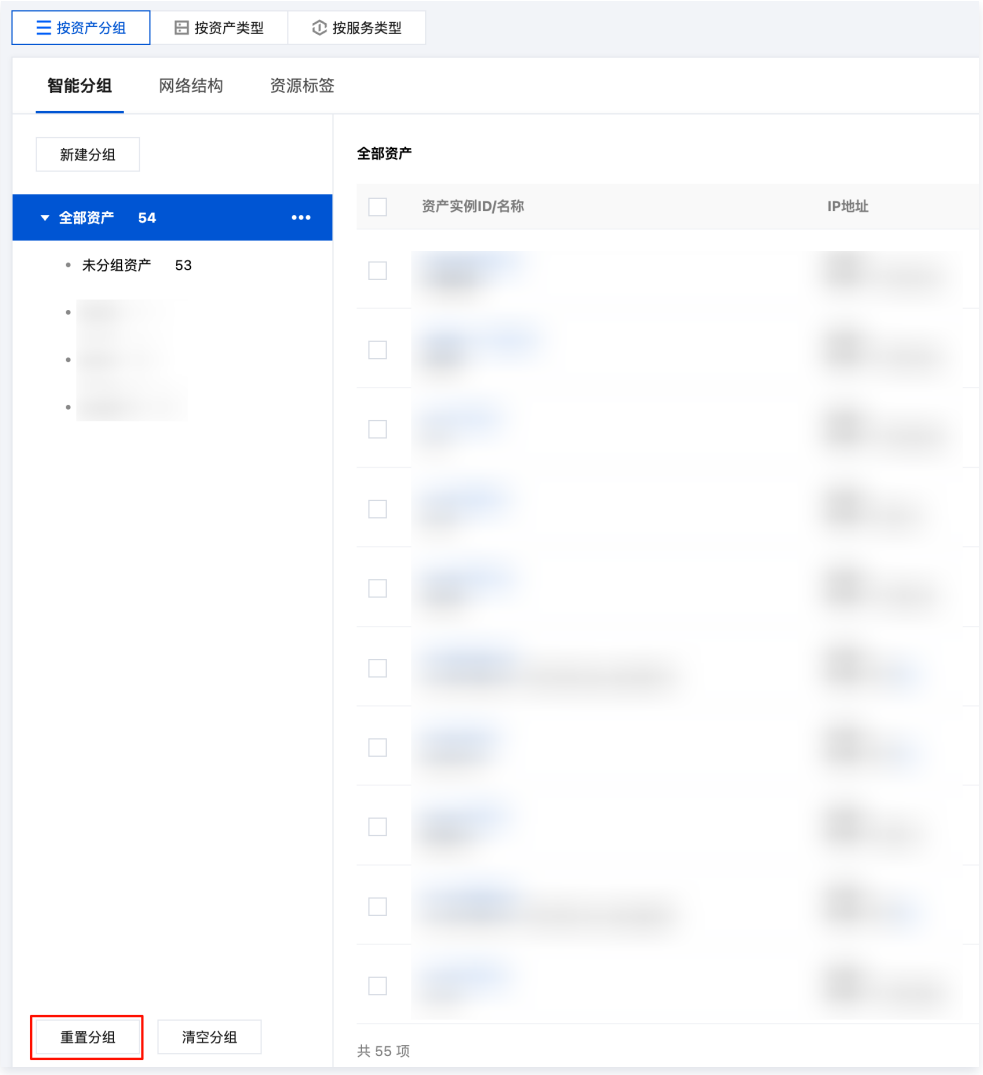
1. 在 资产中心 > **按资产分组** > **智能分组**页面，单击分组的...图标，单击**编辑分组名称**。



2. 在编辑资产分组弹窗中，修改父分组。
3. 可在分组名称栏中进行编辑，单击**确定**，完成编辑。

重置分组

1. 在 资产中心 > **按资产分组** > **智能分组**页面，单击页面左侧最下方的**重置分组**。



2. 在“确认重置”弹窗中，单击**确定**，等待一段时间即可重置分组。

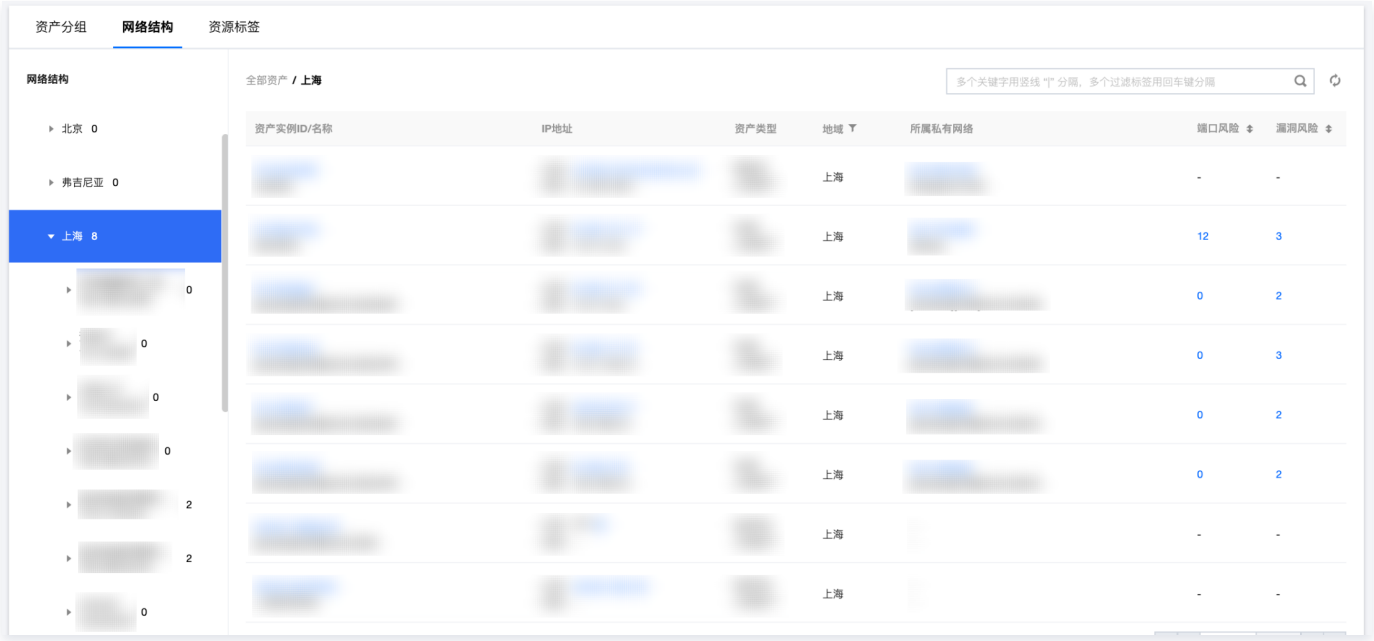
> **注意**
> 若当前资产分组有被用于安全策略的配置则不可重置，请手动删除所有规则后再尝试操作。

网络结构

网络结构页面，支持用户对不同地域下的资产进行查看，当前支持的地域包括国内所有地域与部分海外地域。

1. 在 资产中心 > **按资产分组** > **网络结构**页面，单击左侧的**地域列表**，查看该地域下的所有资产信息。

2. 单击单个地域左侧的 ▸，显示该地域下的所有 VPC 信息，每个 VPC 后显示该 VPC 下的资产数量。单击 **VPC 名称**，可显示该 VPC 下的资产详情。



资源标签

资产标签栏支持通过标签的方式对资产进行管理。

1. 在 资产中心 > **按资产分组** > **资源标签**页面，单击左侧的**标签列表**，查看该标签下的所有资产信息。

2. 单击单个标签键左侧的 ▸，显示该标签键下的所有标签值信息，每个标签值后显示该标签值下的资产数量。单击**标签值**，可显示该标签值之下的资产详情。

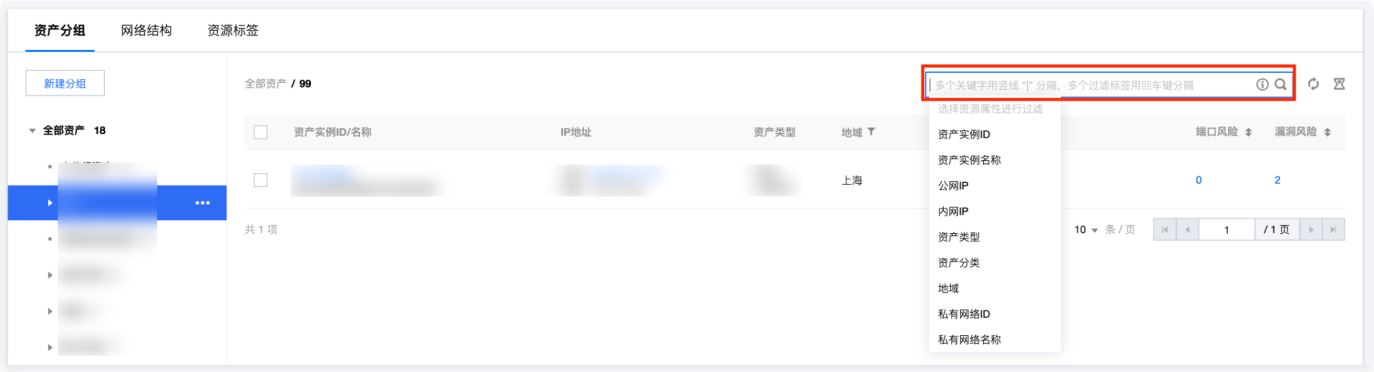
3. 单击**资产名称**，跳转至资产详情页，单击资产标签的 ✎，可以编辑资产的标签信息。

筛选并查看目的资产

1. 用户可以根据业务需求，单击资产分组实例列表中的地域，对资产进行地域筛选。

2. 单击**端口风险**、**漏洞风险**，可将资产按升序或降序方式排列。

3. 单击**搜索框**，可根据关键字对资产进行搜索。



资产列表

最近更新时间：2025-06-30 11:53:01

登录 云防火墙控制台，在左侧导航中，单击**资产中心** > **按资产类型**，进入资产列表页面。资产列表展示了六种不同类型资产的详细信息，包括主机资产、公网 IP 资产、域名资产、网络资产、数据库资产类型，具体资产分类详见下表。

资产分类	子分类	英文名称	中文名称
主机	-	CVM	云服务器 CVM
		LH	轻量应用服务器
		CPM	黑石服务器
		ECM	边缘计算器
		OTHER	其他
公网 IP	-	HAVIP	高可用虚拟 IP
		EIP	弹性公网 IP
		IP	公网 IP
域名	-	DOMAIN	域名
网络	网关	NAT	NAT 网关
		VPN	VPN 网关
	网卡	ENI	弹性网卡
	私有网络	VPC	私有网络
	子网	SUBNET	子网
数据库	-	MySQL	云数据库 MySQL
		REDIS	云数据库 Redis
		MARIADB	云数据库 MariaDB
		PostgreSQL	云数据库 PostgreSQL
		MangoDB	云数据库 MangoDB
其他	-	CLB	负载均衡 CLB
		NATFW	NAT 防火墙
		PROBE	探针

查看资产详细信息

资产详情

1. 在资产列表中，单击**目标资产实例 ID**，即可跳转到该资产的详情页面。

2. 以主机资产为例。在主机资产详情页面，页面左侧可以查看该资产的详细信息，包括资产实例名称、防护情况、IP 地址、资源标签等信息。页面右侧，可以查看该资产的指纹统计、风险趋势、网络攻击趋势的图形化信息。

3. 在页面下方，可以查看该主机资产的风险管理与网络攻击信息。

资产风险管理

> **注意**
> 默认显示未处理过的风险信息。

端口风险

1. 对于未处理的端口风险，单击操作列的**封禁端口**，支持下发访问控制规则，拦截目标端口的访问。封禁后，该风险的处理状态置为已封禁。

2. 防御处置后的风险可以单击操作列的**更多> 标记处置**，表示该风险已被处理，该风险的处理状态置为标记已处置。

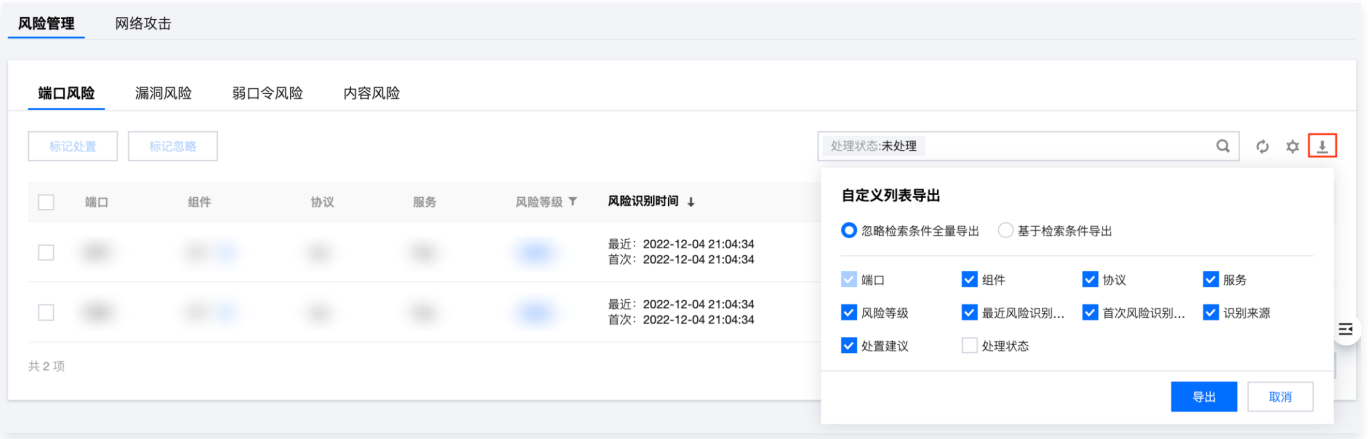
> **注意**
> 当下次扫描任务中仍然检测到此风险，则处理状态重新变回未处理。

3. 当扫描误报产生风险误报时或认为该风险无需处理时，单击操作列的**更多 > 标记忽略**，可将该风险忽略，后续扫描任务中该风险将被过滤。

4. 标记处置与忽略支持批量操作，选择多个风险，单击左上角的**标记处置**或**标记忽略**。

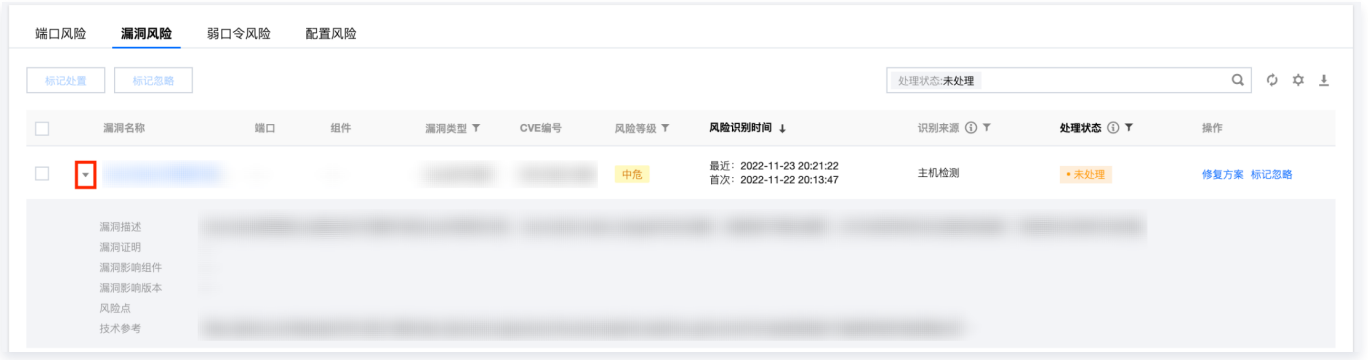
5. 单击⚙图标，可自定义风险列表字段，显示用户关注的风险信息。

6. 单击图标，可导出风险列表，支持自定义导出字段以及检索条件。



漏洞风险

1. 在漏洞风险页签中，单击，可查看漏洞具体详情，包括漏洞描述等。



2. 对于未处理的漏洞风险，单击操作列的**修复方案**，支持查看腾讯威胁情报提供的漏洞修复方案以及对应的参考链接。

3. 标记处置与忽略操作，参见 端口风险 。
4. 自定义风险列表与导出风险列表操作，参见 端口风险 。

弱口令风险

1. 弱口令风险显示对应的弱口令类型与服务，用户可以进行标记处置与忽略操作，参见 端口风险 。
2. 自定义风险列表与导出风险列表操作，参见 端口风险 。

3.

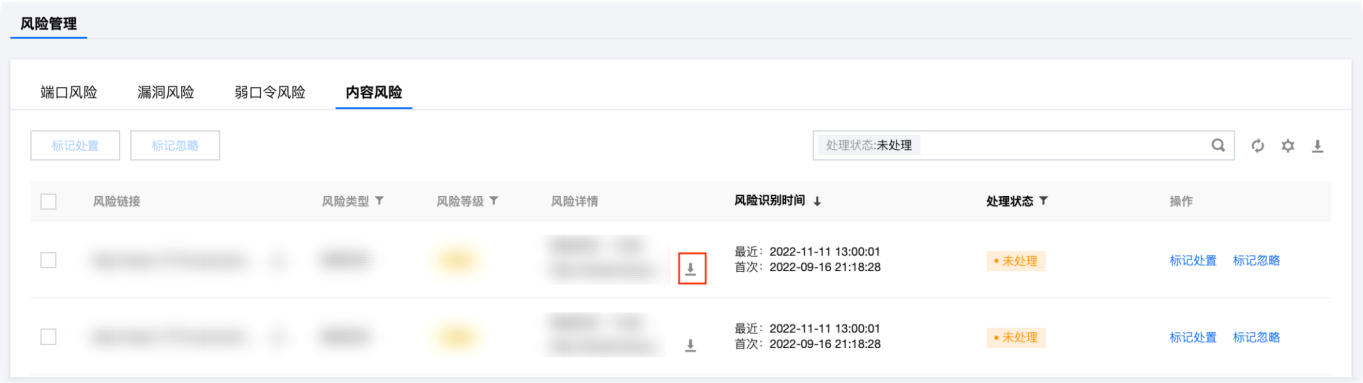
配置风险

1. 在配置风险页签中，单击 ▸，可查看配置风险具体详情，包括风险说明等。

2. 标记处置与忽略操作，参见 端口风险 。
3. 自定义风险列表与导出风险列表操作，参见 端口风险 。

内容风险

1. 内容风险包括敏感信息、挂马暗链、网页篡改三类网站内容风险，显示风险所在的网站链接。单击风险详情列中的 ⬇，可以下载该网站 html 源文件内容进行查看。



> ⚠ **注意**
> 公网 IP 资产、域名资产特有的风险类型，表示该 IP/域名下的网站内容风险。

2. 标记处置与忽略操作，参见 端口风险 。
3. 自定义风险列表与导出风险列表操作，参见 端口风险 。

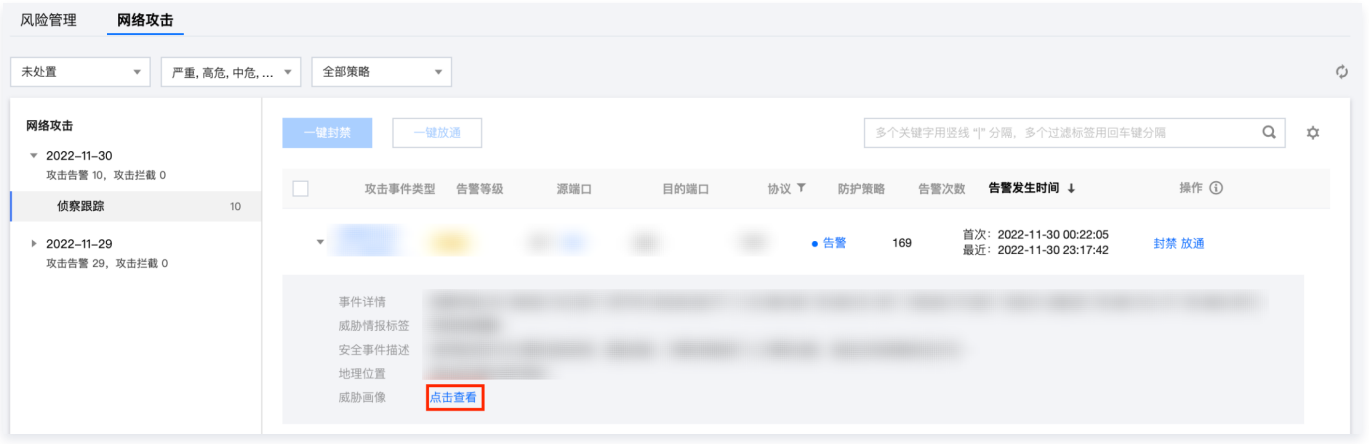
资产网络攻击

以时间为顺序记录了该资产发生的网络攻击告警与拦截事件。

1. 用户可以根据①**事件处置状态（默认为未处置）**、②**告警等级**、③**执行策略**、④**搜索框关键字**对网络攻击事件进行筛选。

2. 选中具体事件，单击 ▸，可查看事件详情，包括事件描述、威胁情报标签等。

3. 单击**威胁画像 > 点击查看**，可以查看攻击 IP 的威胁画像信息。



4. 支持对攻击事件的相关 IP 进行一键封禁。单击①**处的封禁**，可以拦截单个 IP 对全部资产的访问。选中多个事件，单击②**中的一键封禁**，可以对选中的多个 IP 进行拦截。

5. 对于事件中可能存在的重复或误报，支持对相关 IP 进行一键放通。单击①**处的放通**，可以对单个 IP 的流量放行。选中多个事件，单击②**中的一键放通**，可以对选中的多个 IP 流量进行放行。

> **说明**
> 关于封禁与放通攻击 IP 操作，详情可参见 告警中心 文档。

6. 单击⚙图标，可自定义事件列表字段，显示用户关注的事件信息。

主机资产

主机资产统计概况

1. 查看资产统计概况，页面左侧包括主机资产、未防护主机、风险主机、公网主机、内网主机个数，单击**数字**，页面下方即可筛选对应主机资产列表，供用户查看资产详情。
2. 用户可以在页面右侧查看对应时间段内，网络攻击告警、攻击拦截、暴露端口、暴露漏洞统计的 TOP5 资产。

> **注意**
> 暴露端口、暴露漏洞数据需要在资产扫描完成后，根据扫描结果生成。

查看主机资产列表

1. 用户可以在页面下方，根据①**防护状态**、②**风险状态**、③**创建时间**、④**搜索框**关键字筛选对应资产。

> **说明**
> 防护状态指主机安全产品下的防护状态。若用户未安装主机安全，单击操作列的**立即安装**，可安装主机安全客户端。若用户已安装主机安全，单击操作列的**防护详情**，可进入主机安全控制台查看防护详情。

2. 单击 图标，可筛选对应的资产信息，包括 IP 地址、资产类型、地域、所属私有网络。

3. 单击 图标，可对相应信息进行资产排序，包括入/出向峰值带宽、网络攻击、暴露端口、暴露漏洞、配置风险、恶意主动外联、扫描任务、时间。

> **注意**
> 暴露端口、暴露漏洞、配置风险数据需要在资产扫描完成后，根据扫描结果显示。

4. 单击图标，支持用户自定义资产列表内容。

5. 单击图标，可以导出资产列表，支持自定义列表内容与检索条件。

公网 IP 资产

公网 IP 资产统计概况

1. 查看资产统计概况，页面左侧包括公网 IP 资产、未防护公网 IP、风险公网 IP、绑定 CVM 资产、绑定 CLB 资产、绑定 NAT 资产，单击**数字**，页面下方即可筛选对应公网 IP 资产列表，供用户查看资产详情。
2. 用户可以在页面右侧查看对应时间段内，入/出向峰值带宽、入/出向累计流量、网络攻击告警、攻击拦截、暴露端口、暴露漏洞统计的 TOP5 资产。

> **注意**
> 暴露端口、暴露漏洞数据需要在资产扫描完成后，根据扫描结果生成。

查看公网 IP 资产列表

1. 用户可以在页面下方，根据①**防护状态**、②**风险状态**、③**创建时间**、④**搜索框**关键字筛选对应资产。

> **说明**
> 防护状态指是否使用云防火墙进行相关防护，包括已防护、未防护、未知三种状态。若用户未开启云防火墙，单击操作列的**开启防护**，可开启互联网边界防火墙开关，为此公网 IP 资产的访问流量进行防护。若用户已启用防火墙开关，单击操作列的**防护详情**，可跳转至入侵防御模块，查看防火墙防护模式。

2. 单击 图标，可筛选对应的资产信息，包括公网 IP 类型、资产归属、地域。

3. 单击 图标，可对相应信息进行资产排序，包括入/出向峰值带宽、网络访问、网络攻击、端口风险、漏洞风险、弱口令风险、内容风险、时间。

> **注意**
> 暴露端口、暴露漏洞、弱口令风险、内容风险数据需要在资产扫描完成后，根据扫描结果显示。

4. 自定义资产列表内容与导出资产列表信息，参考主机资产。

域名资产

域名资产统计概况

1. 查看资产统计概况，页面左侧包括域名资产、未防护域名资产、风险域名资产、绑定 CVM 资产、绑定 CLB 资产，单击**数字**，页面下方即可筛选对应域名资产列表，供用户查看资产详情。
2. 用户可以在页面右侧查看对应时间段内，网络访问次数、BOT 访问次数、网络攻击告警、攻击拦截、暴露端口、暴露漏洞统计的 TOP5 资产。

> **注意**
> 暴露端口、暴露漏洞数据需要在资产扫描完成后，根据扫描结果生成。

查看域名资产列表

1. 用户可以在页面下方，根据①**防护状态**、②**风险状态**、③**创建时间**、④**搜索框**关键字筛选对应资产。

> **注意**
> 防护状态指是否使用 Web 应用防火墙（WAF）产品进行防护，包括已防护、未防护两种状态。若用户未开启 WAF 防护，单击操作列的**开启防护**，可开启 WAF，为此域名资产的访问流量进行防护。若用户已启用 WAF 防护，单击操作列的**防护详情**，可跳转至 Web 应用防火墙查看防护详情。

2. 单击 图标，可筛选对应的资产信息，包括资产归属、地域、关联实例类型。

3. 单击 图标，可对相应信息进行资产排序，包括网络访问、BOT 访问、网络攻击、端口风险、漏洞风险、弱口令风险、内容风险、扫描任务。

> **注意**
> 暴露端口、暴露漏洞、弱口令风险、内容风险数据需要在资产扫描完成后，根据扫描结果显示。

4. 自定义资产列表内容与导出资产列表信息，参见 主机资产 。

网络资产

网络资产统计概况

1. 查看资产统计概况，页面左侧包括网络资产、网关资产、网卡资产、私有网络、子网，单击**数字**，页面下方即可筛选对应域名资产列表，供用户查看资产详情。
2. 用户可以在页面右侧查看对应时间段内资产类型分布信息、以及入/出向峰值带宽、入/出向累计流量、网络攻击告警、攻击拦截、暴露端口、暴露漏洞统计的 TOP5 资产。

> **注意**
> 暴露端口、暴露漏洞数据需要在资产扫描完成后，根据扫描结果生成。

查看网络资产列表

1. 网络资产划分为网关、网卡、私有网络、子网四种类型，可根据①**风险状态**、②**创建时间**、③**搜索框**关键字筛选对应资产。

> **注意**
> 风险状态需要对资产扫描后的风险情况进行筛选，私有网络资产不支持资产扫描。

2. 单击 图标，可筛选对应的资产信息，如 IP 地址、资产类型、地域等。

3. 单击 图标，可对相应信息进行资产排序，如网络攻击、端口风险等。

> **注意**
> 风险数据需要在资产扫描完成后，根据扫描结果显示。

4. 自定义资产列表内容与导出资产列表信息，参见 主机资产 。

数据库资产

数据库资产统计概况

1. 查看资产统计概况，页面左侧包括数据库资产、未防护数据库、风险数据库，单击**数字**，页面下方即可筛选对应域名资产列表，供用户查看资产详情。

2. 用户可以在页面右侧查看对应时间段内资产类型分布信息、以及数据库访问量统计的 TOP5 资产。

> **注意**
> 风险数据需要在资产扫描完成后，根据扫描结果生成。

查看数据库资产列表

1. 用户可根据①**风险状态**、②**创建时间**、③**搜索框**关键字筛选对应资产。

2. 单击**接入域名管理**，可跳转至**零信任防护 > 接入域名管理**，可为数据库资产接入域名，使用微信扫码登录功能进行资产防护。
3. 单击 图标，可筛选对应的资产信息，包括资产类型、地域、所属私有网络。

4. 单击 图标，可对相应信息进行资产排序，包括网络访问、网络攻击、配置风险、扫描任务。

> **注意**
> 风险数据需要在资产扫描完成后，根据扫描结果显示。

5. 自定义资产列表内容与导出资产列表信息，参见 主机资产 。

服务梳理

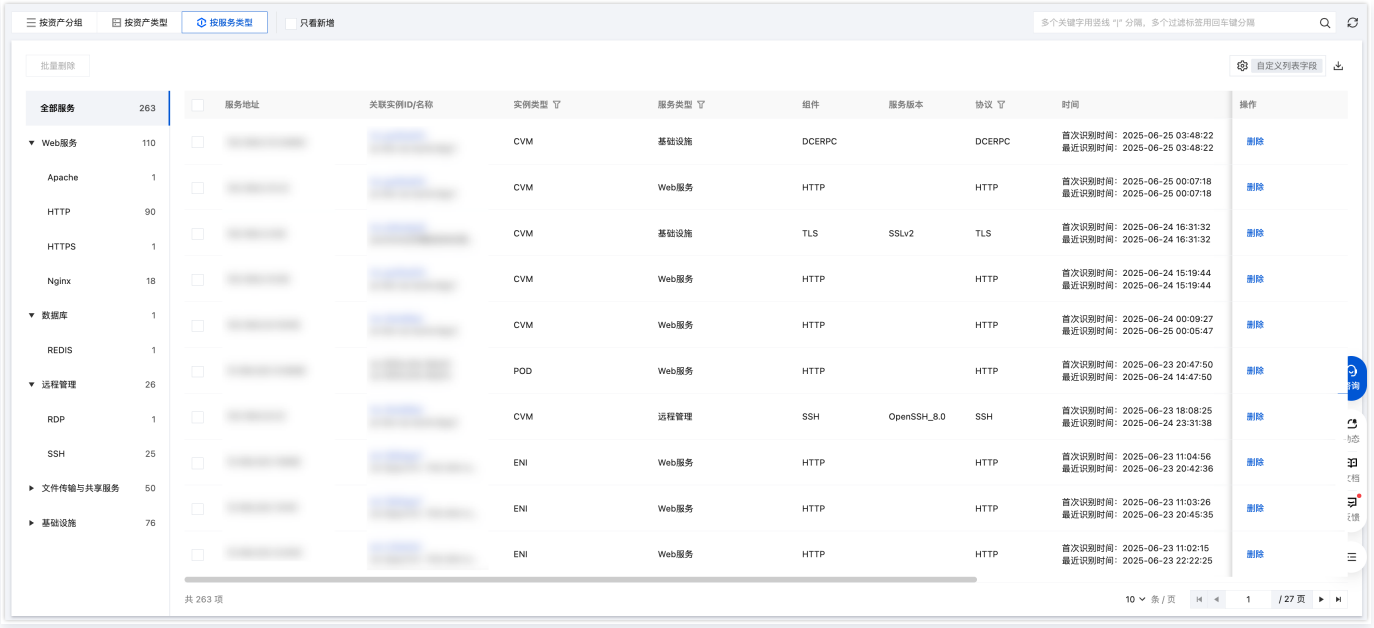
最近更新时间：2025-06-30 11:53:01

版权所有：腾讯云计算（北京）有限责任公司

通过全流量检测与响应 NDR 自动识别网络资产，精准识别资产组件及服务类型，建立资产清单，助企业了解资产状况，避免遗漏与管理盲区。采用被动识别方式，对业务无侵入。

> **注意：**
> - 按服务类型识别资产功能需要购买全流量检测与响应 NDR。
> - 提交工单 申请试用全流量检测与响应 NDR 功能。

1. 登录 云防火墙控制台，在左侧导航中，单击**资产中心 > 按服务类型**。
2. 在按服务类型页面，支持识别服务类型、组件、服务版本、协议等信息；支持被动识别资产服务类型，包含 Web 服务、数据库、远程管理、文件传输与共享服务、基础设施等。
3. 在按服务类型页面，单**击实例 ID**，可查看 资产详情 。



告警中心
概述

最近更新时间：2025-06-30 11:53:01

告警中心统计了入侵防御模块和网络蜜罐模块检测到的网络攻击与风险事件，了解防火墙防护状况，从而及时预警，支持对危险访问源进行封禁。按照防火墙执行的动作，分为攻击告警汇总、攻击拦截统计、攻击欺骗事件。

- 攻击告警汇总：包含了所有检测到的观察类型的网络攻击与风险事件（需要用户手动进行攻击 IP 封禁/放通/隔离/忽略）。
- 攻击拦截统计：包含了对所有检测到威胁并自动拦截的网络攻击与风险事件（用于后续审计与排查）。
- 攻击欺骗事件：包含了对所有检测到的暴露探针和蜜罐的网络攻击与风险事件（可手动设置封禁或通行）。

版本支持说明

云防火墙所有版本均支持告警中心功能，计费详情请参见 计费概述 。

相关文档

- 旧版告警中心请参见以下文档：
  - 告警事件查看与处理
  - 拦截事件查看与处理
  - 欺骗事件查看与处理
- 新版告警中心请参见文档： 攻击告警事件查看与处理 。

版权所有：腾讯云计算（北京）有限责任公司

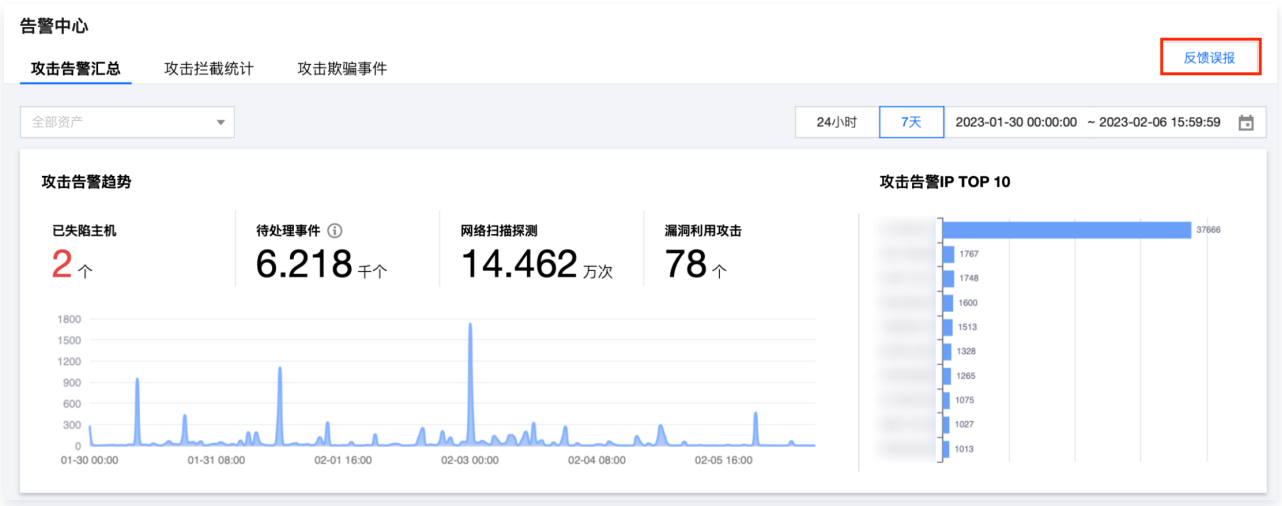
反馈误报

最近更新时间：2024-05-17 15:49:31

当规则告警信息，出现误报情况时，用户可以在 告警中心 的反馈误报入口进行误报上报，从而及时从告警信息处提交反馈。

方式一

1. 当发现告警信息出现误报时，单击**反馈误报**，提交误报信息。



2. 在反馈误报页面，选中反馈类型，填入对应的误报信息，包括：
   2.1 IP/域名：需要填入误报的 IP 地址或域名，以及误报描述。
   2.2 入侵防御规则：需要填入误报的规则 ID，以及误报描述。

> **注意：**
> 可通过告警事件详细信息中，查看事件命中规则详情，从而快速获得误报事件对应的规则 ID。

3. 单击**提交反馈**，即可完成误报反馈。误报反馈记录将在页面下方进行展示，云防火墙工作人员会在3个工作日内完成评估并反馈处理结果。

方式二

1. 当发现告警信息出现误报时，单击操作栏中的**放通**，将误报 IP 地址加入 入侵防御 模块的放通列表（白名单）。

2. 在弹窗中选择勾选放通原因为**误报**，并选择上报误报地址/规则。在下方填写误报描述后，单击**确定**即反馈成功。

3. 误报反馈记录将在页面下方进行展示，云防火墙工作人员会在3个工作日内完成评估并反馈处理结果。

攻击告警事件查看与处理

最近更新时间：2025-06-30 11:53:01

> **说明：**
> 告警中心全新版本上线，本文档仅针对新版告警中心操作进行说明。如果您当前使用旧版告警中心，可以在告警中心右上角单击**前往新版**进行切换。

攻击告警事件按攻击类型、攻击手法、资产影响程度等维度将用户入侵防御日志聚合展示，支持趋势分析、告警处置及详情查看。用户可按多条件筛选告警，执行封禁、放通、隔离等操作。

查看攻击告警趋势

攻击告警趋势提供 TOP 10观察事件 IP、受影响资产等关键指标统计，并可视化呈现事件趋势，支持单击**快捷筛选**，实现攻击溯源与处置闭环。通过告警信息的可视化汇总，可以方便地对防火墙监测到的攻击事件进行统计分析与操作处置，统计数据每20分钟更新一次。

1. 登录 云防火墙控制台，在左侧导航中，单击**告警中心 > 攻击告警事件**。
2. 在攻击告警事件页面左上角选择时间，对该范围中的安全告警事件进行分析。
3. 在攻击告警趋势中，可以查看以下模块：

模块	说明	交互功能
待处理事件	当前未被处置的中高风险观察类告警，反映当前最紧迫的安全风险。	单击**数字**筛选相关告警，建议优先处理。
主机失陷事件	标识确认被攻陷的资产，提示内网横向扩散风险。	单击**数字**筛选相关告警，建议进行隔离操作。
高危告警	综合判定对业务存在重大风险，需要关注并及时处理。	单击**数字**筛选相关告警，建议及时修复相关风险。
攻击告警趋势图	以折线图展示“观察”和“拦截”动作的告警数量随时间变化趋势。	支持单击切换图例显示，辅助分析攻击高峰期。
观察事件 IP TOP 10	观察事件中攻击 IP 的 TOP 统计。	• 单击 IP 支持快捷复制。 • 单击**柱状图**支持快捷筛选。
受影响资产 TOP 10	除“恶意 IP 攻击”类型之外所有攻击中受影响资产的 TOP 统计。	• 单击 ID 支持快捷复制。 • 单击**柱状图**支持快捷筛选。

处置告警事件

在告警列表中支持按事件等级（高/中/低危）、流量方向、攻击结果等多条件筛选攻击告警事件。用户可对近7天内的告警单条或批量执行封禁、隔离、加白、忽略等操作，并联动日志审计追溯攻击详情。

> **说明：**
> • 告警中心仅支持操作近 7 天内的告警事件。
> • 对指定目标进行处置后，处置状态会修改为已处置，同时移动至对应已处置的告警事件中。

功能分类		

筛选与搜索	快捷筛选	支持按处置状态、防护动作快速过滤告警。
	高级搜索	支持 IP、实例 ID、事件等级、攻击阶段等多条件组合搜索，多个关键字用竖线“|”分隔。
	自定义列表字段	固定显示攻击类型、访问源、访问目的，其他字段（如首次发生时间、防火墙类型）可自定义显示。
	自定义列表导出	支持全量导出或基于检索条件导出当前选定时间范围的告警事件。
处置操作	封禁	将指定云外 IP 加入入侵防御-封禁列表中，拦截其所有访问请求。
	隔离	自动下发企业安全组阻断规则，拦截指定资产的指定方向的网络访问，可能导致资产断网，需谨慎使用。
	加白	将 IP 加入入侵防御-白名单策略列表中，不再进行入侵防御检测。
	忽略	标记告警为“已忽略”，当天相同攻击事件不再告警，也不会在攻击告警趋势中进行统计。
告警事件查看	告警列表	在告警列表中，可以查看告警事件的相关消息，包括攻击类型、事件等级、攻击阶段、访问源、访问目的、流量方向、策略、首次发生时间、最近发生时间、告警次数、判断来源、防火墙类型、攻击结果、告警分类、处置状态。

	查看详情	在告警列表中，单击操作列的**详情**，可查看告警事件详情。
		• AI 事件解读
		  ○ 事件总结：分析攻击手法及潜在危害。
		  ○ 处置建议：提供操作指导。
		  ○ 推论依据：说明事件等级判定逻辑。
		• 详情功能模块
		  ○ 基本信息：展示攻击类型、事件等级、首次/最近发生时间等。
		  ○ payload 信息：显示攻击请求信息。
		  ○ 访问源视角：展示攻击源 IP、资产类型、地域及关联访问目的。
		  ○ 访问目的视角：展示受影响资产 ID、内网 IP 及关联访问源。

告警聚合规则

告警列表基于入侵防御日志聚合生成，将原始日志按攻击特征和影响范围合并为更清晰的事件条目，减少重复告警干扰。具体聚合规则如下：

事件类型	说明
恶意 IP 攻击事件	所有具有相同处置状态、来自恶意 IP 攻击的告警（无论目标或手法）聚合为一个事件，统一展示威胁来源。
恶意 IP 访问事件	具有相同处置状态、相同访问源 IP 的告警聚合为一个事件，突出失陷主机风险。
恶意域名访问事件	具有相同处置状态、相同访问目的域名的告警聚合为一个事件。
其他类型攻击事件	满足以下全部相同条件的告警聚合为一个事件： • 攻击类型：如 SQL 注入、Web 攻击等。 • 攻击手法：具备相同的 payload 特征。 • 事件等级：告警中心将根据攻击对资产的影响程度，动态调整告警的危险等级为高/中/低危。 • 流量方向：互联网入向/出向、内网访问。 • 策略：云防火墙对攻击会话的处置策略为“观察/拦截”。 • 情报白名单：攻击者信息是否情报白名单。 • 攻击结果：当资产开启全流量检测与响应NDR时，攻击结果为“成功/失败/尝试”；否则为“未知”。 • 处置状态：未处置/已封禁/已加白/已隔离/已忽略。

获取更精确告警研判

当用户资产开启全流量检测与响应（NDR）后，告警中心会根据攻击上下文（如攻击结果、URI 有效性等）动态调整事件等级，使告警事件等级更客观反映真实风险，显著减少误判。同时在告警详情也可以查看更多相关信息，帮助您快速识别和处置真正的高危事件，提升安全运营效率。关于全流量检测与响应（NDR）的详细说明，请参见 全流量检测与响应。

告警事件查看与处理

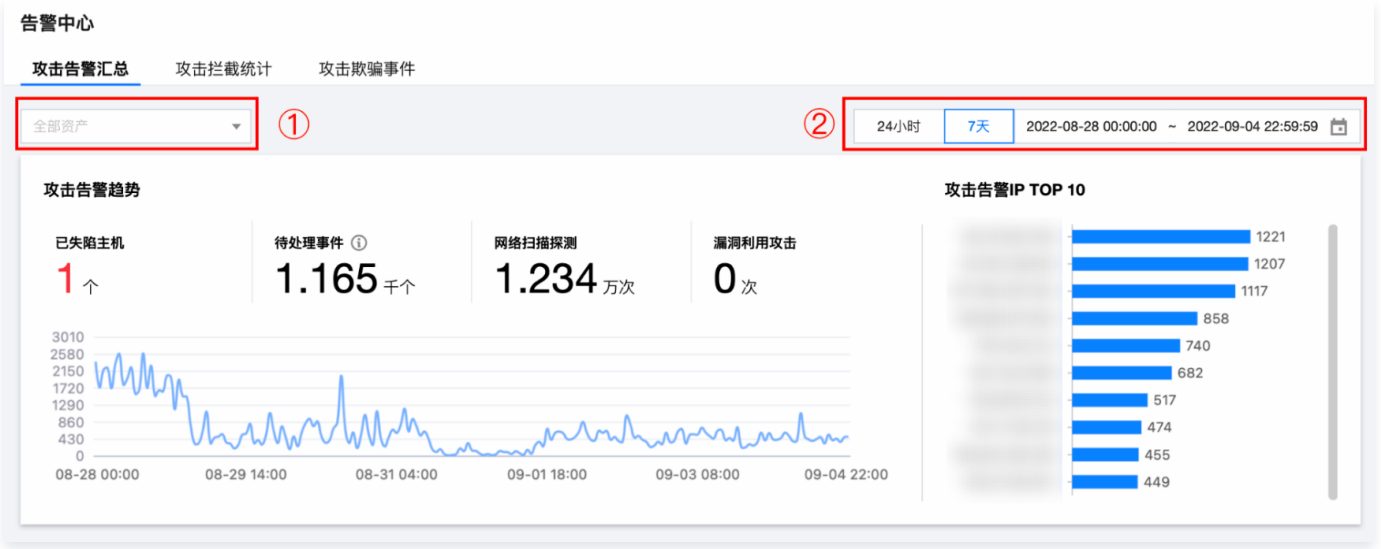
最近更新时间：2025-06-30 11:53:01

> **说明：**
> 告警中心全新版本上线，本文档仅针对旧版告警中心操作进行说明。如果您当前使用旧版告警中心，可以在告警中心右上角单击**前往新版**进行切换。新版告警中心相关内容请参见 攻击告警事件查看与处理 。

攻击告警汇总可视化

通过告警信息的可视化汇总，可以方便地对防火墙监测到的攻击事件进行统计分析与操作处置，统计数据每20分钟更新一次。

1. 登录 云防火墙控制台，在左侧导航中，单击**告警中心** > **攻击告警汇总**。
2. 在攻击告警汇总页面，根据①**个人资产**、②**时间**对已有的安全告警事件进行可视化分析。
   a. 页面左侧为筛选后的近期安全事件的变化趋势曲线，展示了不同时间的告警次数。以及已失陷主机、待处理事件、网络扫描探测和漏洞利用攻击次数的统计情况。
   b. 页面右侧展示了攻击告警 IP 前十排行，为提前规避风险 IP 攻击提供参考。



快速定位告警事件

提供多种筛选功能，支持对已有的攻击告警事件进行快速筛选定位。

在 攻击告警汇总页面 的事件列表中，可以根据①**告警事件类型**、②**条件筛选**、③**自定义表头**对已有的攻击告警事件进行定位。

- 告警事件类型：单击图中①处按钮，查看不同分类下的告警信息详情。

> **说明：**
> 当在 访问控制 、入侵防御 、 安全基线 模块配置好云防火墙所需的相关安全策略后，才会显示对应的安全事件类型。

- 条件筛选：单击图中②处按钮对攻击告警事件进行条件筛选。
- 支持查看未处置、已封禁、已放通、已忽略的告警信息。

- 支持根据告警危险等级筛选。
- 支持根据安全事件类型、协议、判断来源筛选。
- 支持直接单击图标对访问源 IP 或访问目的 IP 进行筛选。
- 支持对发生时间、告警次数进行排序查看。
- 支持关键字搜索筛选。包括访问源、源端口、访问目的、目的端口、危险等级、协议、判断来源。
- 自定义表头：单击图中③处的图标可以定义表头字段，最多勾选10个。

查看定位事件详情

定位到具体的攻击告警事件后，单击事件左侧 ▸ 可以查看事件的详细信息。

> **说明：**
> 前往主机安全深度检测功能需要购买 主机安全 。

- 威胁画像：单击**点击查看**，查看该访问源的威胁画像。包括 IP 地理位置、是否属于威胁情报 IP、网络信息、反查域名信息等。
- 资产详情：单击**点击查看**，跳转至**资产中心**，查看被攻击资产详情。

快速处置告警信息

处置单条告警信息

在 攻击告警汇总页面 ，支持对单条告警信息进行处置。在事件操作栏，对访问源进行**封禁**、**放通**、**忽略**、**隔离**操作。

> **说明：**

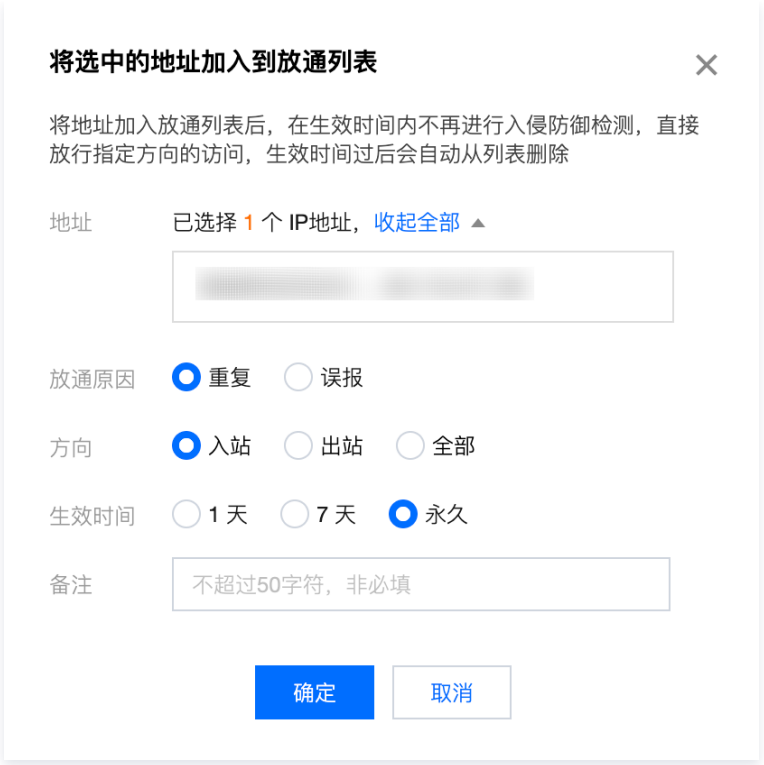
隔离操作仅针对出站方向流量告警事件，隔离失陷主机，防止影响进一步扩大。

- 封禁：针对危险等级较高或告警次数较多的安全事件，可以单击**封禁**，将该 IP 地址添加至 入侵防御 模块的封禁列表（黑名单），并选择封禁时间，添加备注，云防火墙会在时间范围内，自动拦截该 IP 地址对用户全部资产的访问。

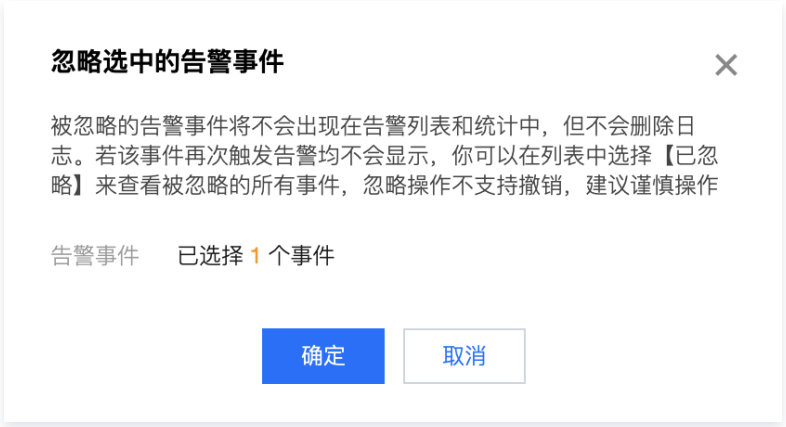
注意：

当告警 IP 地址可能来自情报白名单时，会出现提示信息，请勿手动拦截/封禁，开启入侵防御拦截模式，云防火墙会自动拦截来源于这个地址的攻击流量，并放行正常流量。

- 放通：针对告警中存在重复或可能的误报，可以单击**放通**，将该 IP 地址加入 入侵防御 模块的放通列表（白名单），并选择放通时间与放通原因，填写备注，若是确定为误报，可以对误报内容进行反馈，云防火墙会在一定时间范围内，将该 IP 地址绕过入侵防御模块检测，从而放行该 IP 地址的流量。



- **忽略：如果不想处理告警信息，可以单击忽略，该日志不会消失，但是在处置状态已忽略列表中可以查看记录。**



- **隔离：选择阻断流量方向与生效时间，单击隔离，资产实例隔离会自动下发企业安全组阻断规则，在时间范围内拦截选中资产的指定方向的网络访问。**

说明：

隔离资产实例后，支持使用运维白名单对资产进行访问，可选手动填写 IP 或使用零信任防护两种方式。

- 仅支持手动填写10个 IP。
- 零信任防护支持选择微信或企业微信用户允许进行资产访问，如何接入微信或企业微信用户，详情请参见 企业安全组 。

批量处置告警信息

在 攻击告警汇总页面 ，支持对多条告警信息进行处置。可以选中多条告警信息，单击**一键拦截**、**放通**、**隔离**或**忽略**。

注意：

- 隔离操作仅针对出站方向流量告警事件，隔离失陷主机，防止影响进一步扩大。主要为主机失陷类型告警事件，有隔离操作。
- 用户需要修改操作，可在**入侵防御 > 拦截列表**、**放通列表**或者**隔离列表**中删除该 IP，恢复操作。
- 超出7天告警将会失效，无法处理。

拦截事件查看与处理

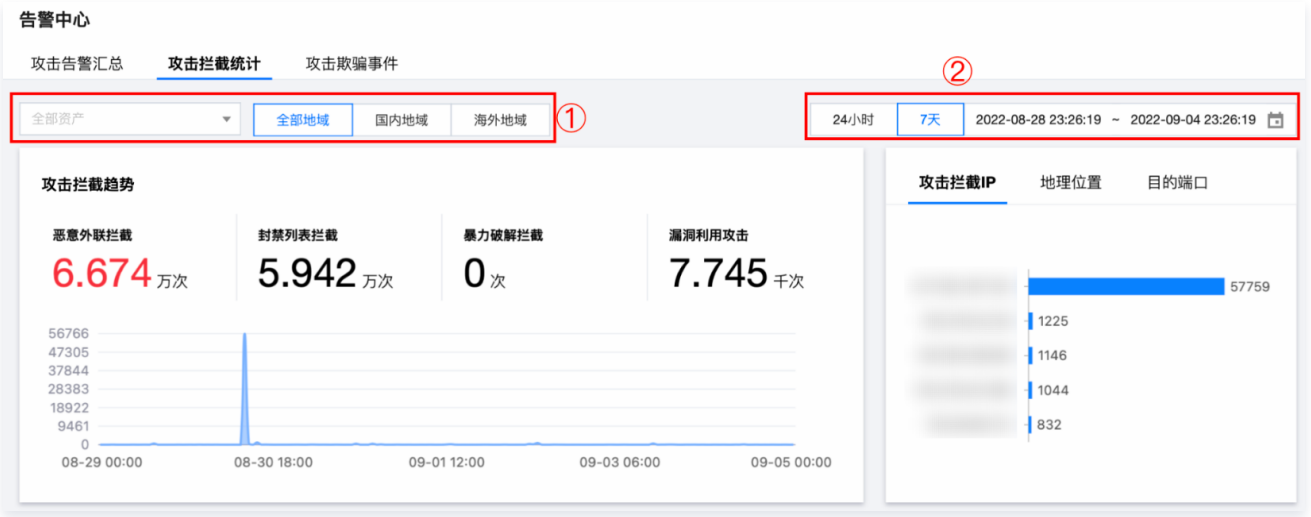
最近更新时间：2025-06-30 11:53:01

> **说明：**
> 告警中心全新版本上线，本文档仅针对旧版告警中心操作进行说明。如果您当前使用旧版告警中心，可以在告警中心右上角单击**前往新版**进行切换。新版告警中心相关内容请参见 攻击告警事件查看与处理 。

攻击拦截统计模块是防火墙基于所有已设置规则和威胁情报等拦截记录的整合，可以帮助对所有已拦截事件进行统计分析和处置，统计数据每20分钟更新一次。

拦截统计可视化

1. 登录 云防火墙控制台，在左侧导航中，单击**告警中心** > **攻击拦截统计**。
2. 在攻击拦截统计页面，支持根据①**个人资产及其地域**、②**时间**对已有的安全告警事件进行可视化分析。
   2.1 页面左侧为筛选后的近期阻断拦截事件的变化趋势曲线，展示了不同时间的拦截次数。以及恶意外联拦截、封禁列表拦截、暴力破解拦截、漏洞利用攻击的统计情况。
   2.2 页面右侧根据攻击拦截 IP、地理位置和目的端口，可以查看拦截事件数量排行榜。



快速定位拦截信息

提供多种筛选功能，支持对已有的攻击拦截信息进行快速筛选定位。

1. 在 攻击拦截统计页面 的事件列表中，提供两种视角展示拦截信息，单击图中**资产视角**或**事件视角**进行视角切换。
   1.1 资产视角会以攻击者资产为视角，将相同访问源的拦截事件合并统计显示。
   1.2 事件视角以独立的拦截事件为视角，将拦截事件一一显示。

> **说明：**
> 以资产视角为例，事件视角可参见 快速定位告警事件 页面。

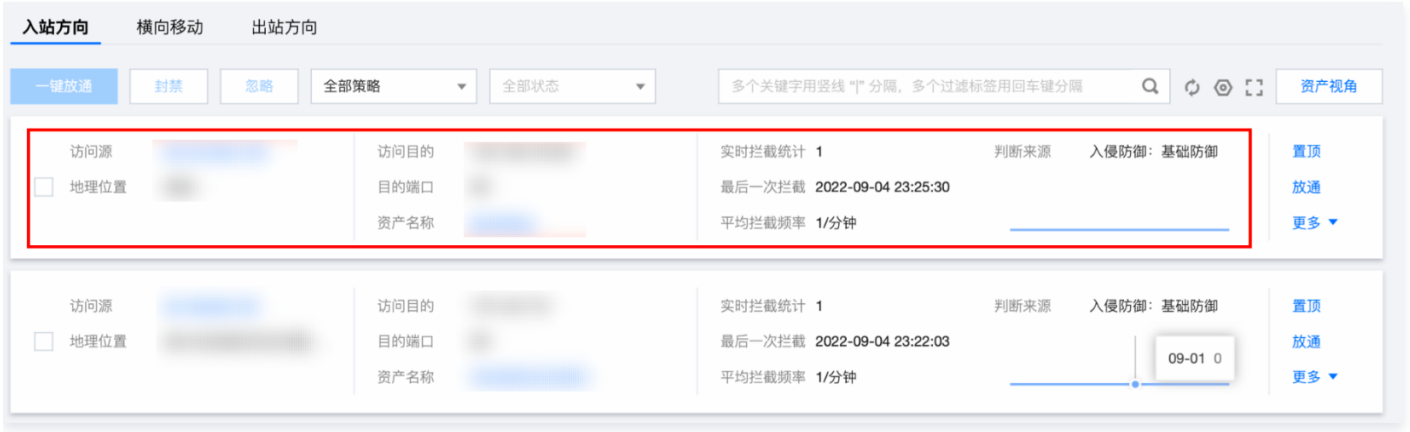
2. 根据①**流量方向**、②**条件筛选**对已有的攻击拦截事件进行定位。

- 流量方向：单击图中①处按钮，查看不同流量方向下的拦截信息详情。包括入站方向、横向移动、出站方向。
- 条件筛选：单击图中②处的 图标对攻击告警事件进行条件筛选。
  - 支持按照入侵防御策略、处置状态显示。
  - 支持按照拦截时间、拦截统计、平均拦截频率排序。
  - 支持以分钟、小时、天作为频率统计。
  - 支持关键字搜索筛选。包括访问源、访问目的、目的端口、地理位置。

查看定位信息详情

在 攻击拦截统计页面 的事件列表中，直接查看拦截信息的信息详情。

> **说明：**
> 以资产视角为例，事件视角可参见 查看定位事件详情 页面。



- 单击**访问源**，查看该访问源的威胁画像。包括 IP 地理位置、是否属于威胁情报 IP、网络信息、反查域名信息等。
- 单击**资产名称**，可跳转至资产中心，查看被攻击资产详情。

快速处置拦截信息

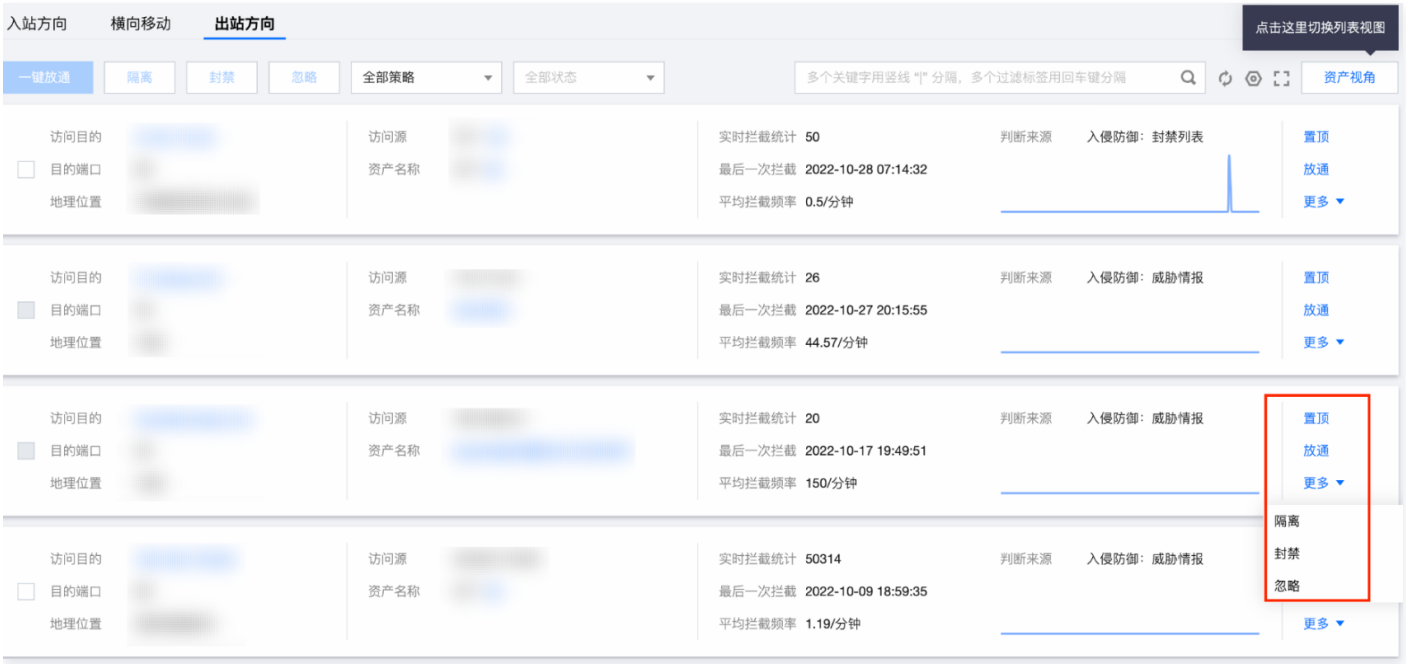
> **说明：**
> 以资产视角为例，事件视角可参考 快速处置告警信息 页面。

处置单条拦截信息

在 攻击拦截统计页面 ，支持对单条拦截信息进行处置。在事件右侧栏处，进行**置顶**、**封禁**、**放通**、**忽略**、**隔离**操作。

> **说明：**

- 由于资产的状态有所不同，因此在右侧的可操作按钮有所不同。隔离操作仅针对横向移动、出站方向拦截事件，隔离失陷主机，防止影响进一步扩大。
- 以下操作同时适用于批量处理和事件视角下的操作。



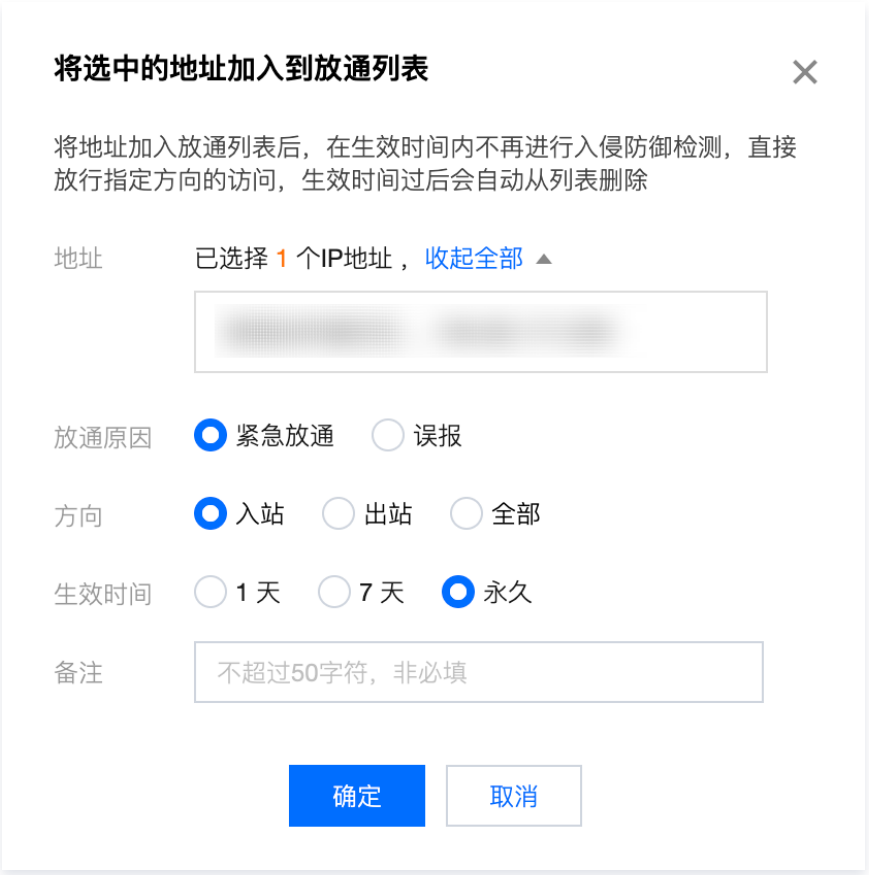
- 置顶：资产视角下，针对发生拦截事件的风险资产，可以一键置顶，方便用户关注资产的实时拦截情况。

> ⚠ **注意：**
> 用户入站方向和出站方向置顶数量最多不可超过5条。

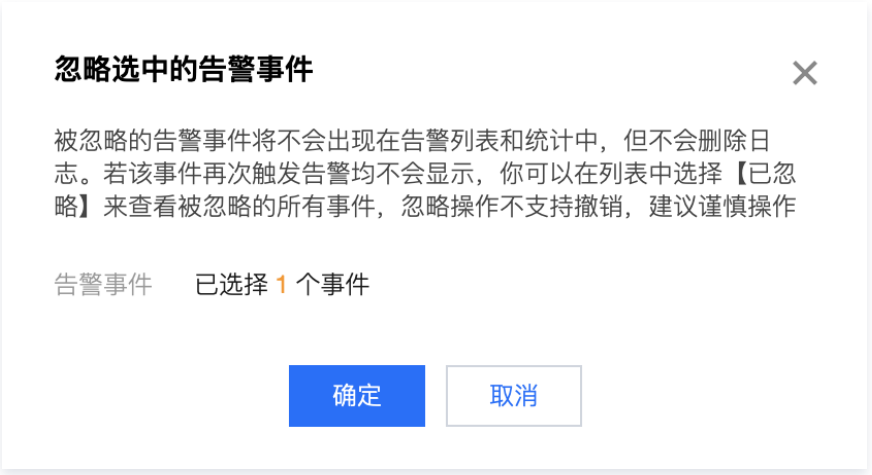
- 封禁：针对危险等级较高的资产，可以单击**封禁**，将该 IP 地址添加至 入侵防御 模块的封禁列表（黑名单），并选择封禁时间，添加备注，云防火墙会在时间范围内，自动拦截该 IP 地址对用户全部资产的访问。

版权所有：腾讯云计算（北京）有限责任公司

- **放通：对于用户任务不应拦截的 IP，可单击放通。将该 IP 地址加入 入侵防御 模块的放通列表（白名单），并选择放通时间与放通原因，填写备注，云防火墙会在一定时间范围内，将该 IP 地址绕过入侵防御模块检测，不再拦截。如果用户不确定放通原因是否为：误报，可优先选择紧急放通，若确定为误报，可以对误报内容进行反馈，单击确定后修改即可。**



- **忽略：针对存在重复的拦截事件，可以单击忽略，被忽略的拦截事件将不会出现在拦截列表和统计中，但不会删除日志。您可以在列表中选择已忽略来查看被忽略的所有事件，忽略操作不支持撤销，建议谨慎操作。**



- **隔离：单击隔离，资产实例隔离会自动下发企业安全组阻断规则，拦截选中资产的指定方向的网络访问，便于后续的定位排查，及时止损。**

> **说明：**
> 隔离资产实例后，支持使用运维白名单对资产进行访问，可选手动填写 IP 或使用零信任防护两种方式。
> - 仅支持手动填写10个 IP。
> - 零信任防护支持选择微信或企业微信用户允许进行资产访问，如何接入微信或企业微信用户，详情请参见 企业安全组 。

批量处置告警信息

在 攻击拦截统计页面 ，支持对多条拦截信息进行处置。可以选中多条拦截信息，单击**一键拦截、放通、隔离或忽略**。

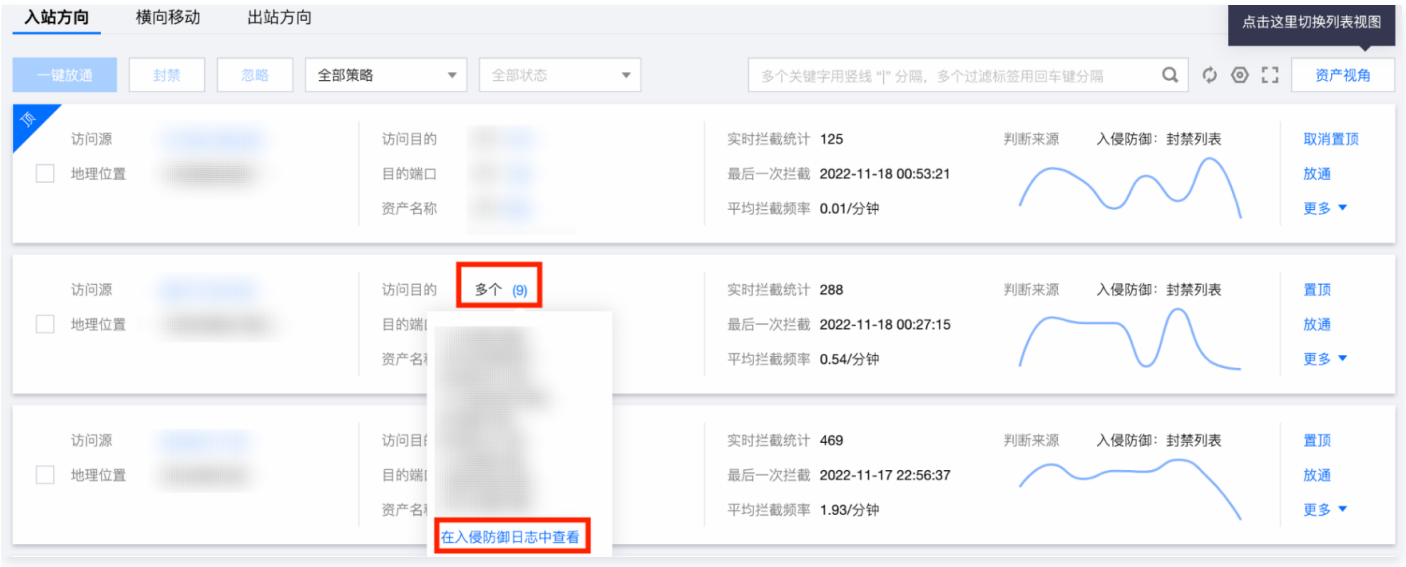
> **注意：**
> - **由于资产的状态不同，因此可操作按钮有所不同。隔离操作仅针对横向移动、出站方向拦截事件，隔离失陷主机，防止影响进一步扩大。**
> - **用户需要修改操作，可在入侵防御 > 拦截列表、放通列表或者隔离列表中恢复操作。忽略操作不支持撤销，建议谨慎操作。**
> - **超出7天告警将会失效，无法处理。**

误报处理

您可以将该 IP 加入白名单中，在攻击拦截统计页面，选择所需资产/IP，单击**放通**，放通原因选择误报，单击**确定**。

查询某 IP 对我的所有攻击事件

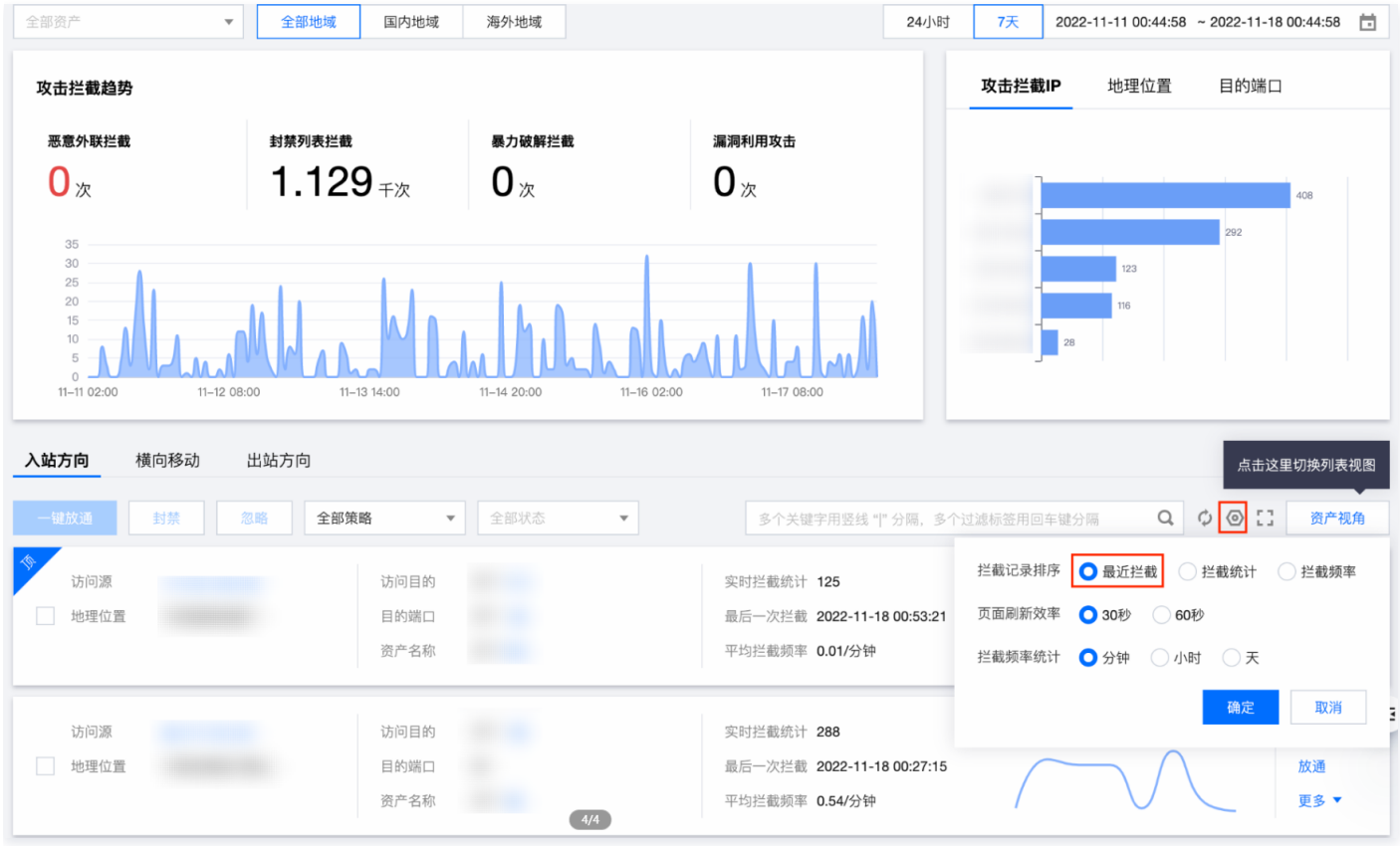
在资产视角下，将鼠标悬浮在**访问目的/访问源**或**资产名称**上，单击下方的在**入侵防御日志中查看**查询所有攻击事件。



说明：
图中以鼠标悬浮**访问目的/访问源**为示例。

查看最新拦截事件

攻击拦截统计页面具有自动刷新功能。在页面上方单击图标，并在拦截记录排序中勾选“最近拦截”，单击**确定**即可实时监控最新拦截事件。



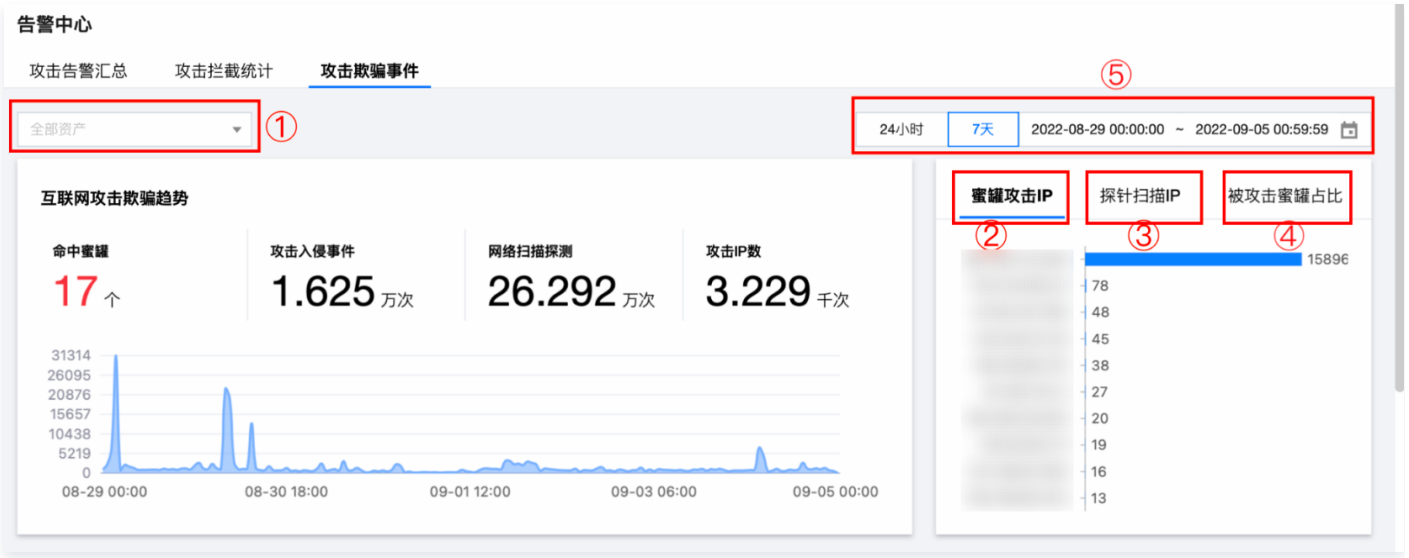
欺骗事件查看与处理

最近更新时间：2024-05-17 15:49:31

欺骗趋势可视化

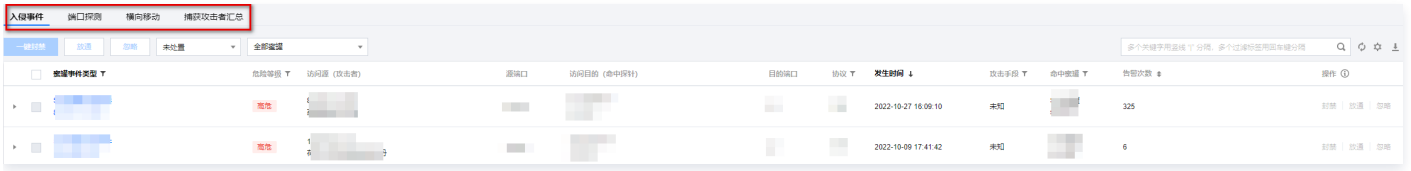
攻击欺骗事件页面可以根据可视化统计和列表式统计，对所有已设置的暴露探针和 网络蜜罐 的扫描和攻击行为进行记录和整合，从而对所有已拦截事件进行统计分析和处置，统计数据每20分钟更新一次。

1. 登录 云防火墙控制台，在左侧导航中，单击**告警中心 > 攻击欺骗事件**。
2. 在攻击欺骗事件页面，支持根据①**探针资产**、②**蜜罐攻击 IP**、③**探针扫描 IP**、④**被攻击蜜罐占比**和⑤**时间**统计并进行可视化分析，在页面左侧查看不同探针或全部探针在不同时间段的命中蜜罐数，攻击入侵事件数，网络扫描探测次数和攻击 IP 的次数。



查看欺骗事件与攻击者信息

在 攻击欺骗事件页面 的事件列表中，有如下攻击欺骗事件类型：

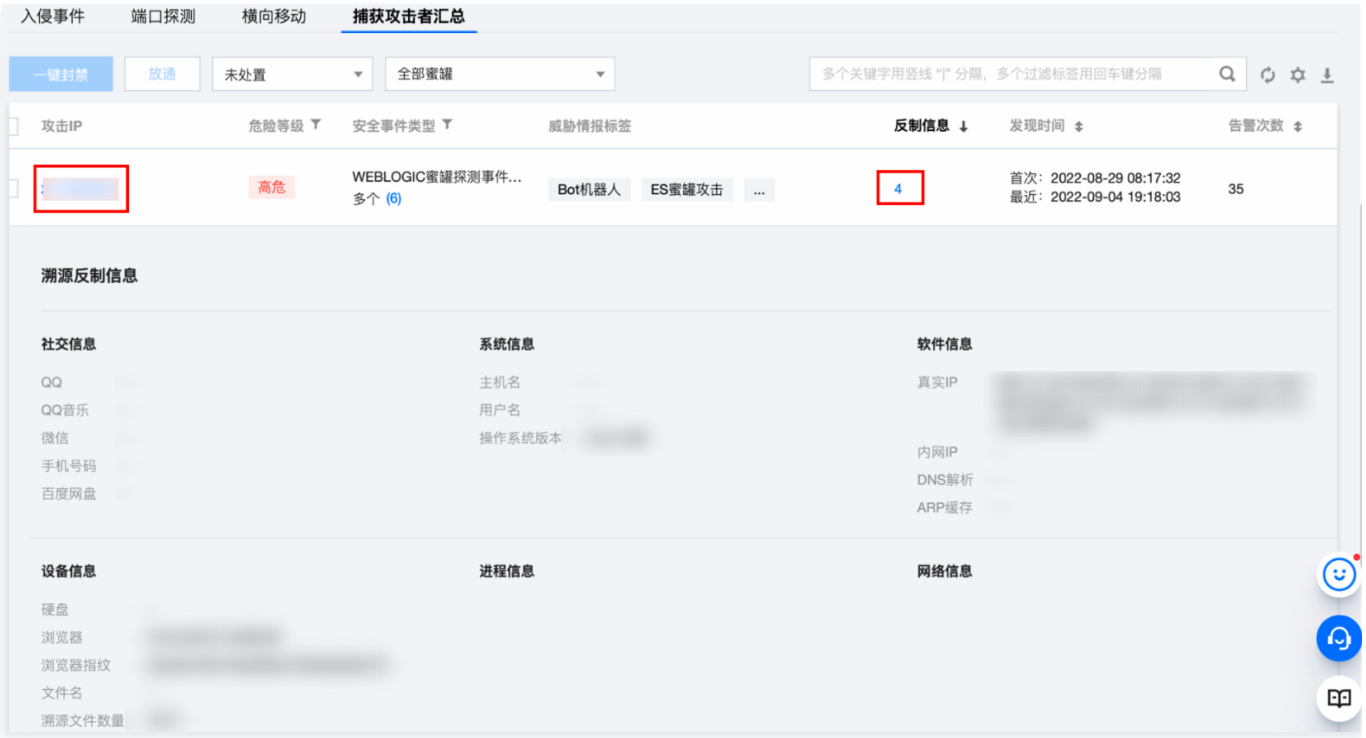


- 入侵事件：攻击事件会导致主机失陷。
- 端口探测：攻击者对蜜罐进行的扫描攻击事件。
- 横向移动：在资产间横向移动的攻击欺骗事件。

> **说明：**
> 对入侵事件、端口探测、横向移动的欺骗事件进行定位查看，支持对蜜罐进行筛选，其余筛选内容可参见 快速定位告警事件 页面。

- 捕获攻击者汇总：对欺骗事件的攻击 IP 信息进行汇总。
  - 支持对威胁等级、安全事件类型对攻击者进行筛选。
  - 支持查看攻击者的威胁情报标签，支持对反制信息、发现事件、告警次数的排序统计。

- 单击**攻击者 IP** 或反制信息栏中的**数字**，可查看该攻击 IP 的溯源反制信息。



快速处置欺骗信息

处置单条拦截信息

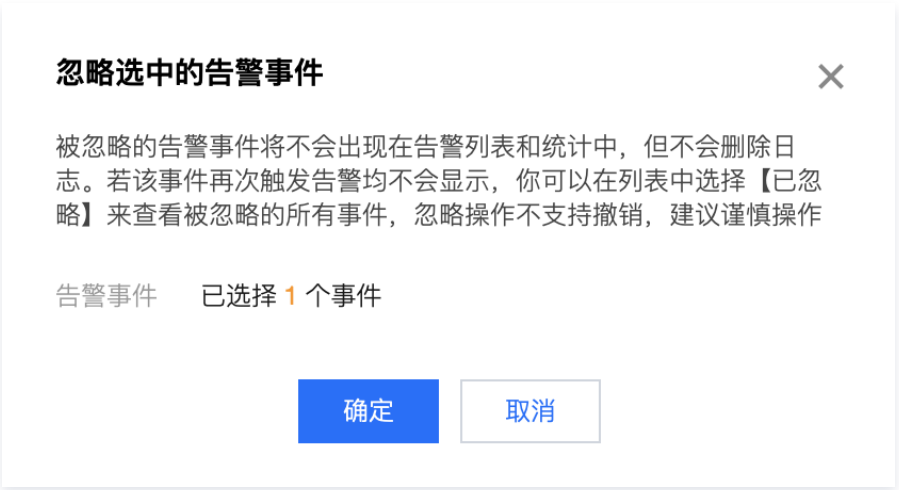
在 攻击欺骗事件页面，支持对单条欺骗事件信息进行处置。在事件右侧栏处，进行**封禁**、**放通**、**忽略**、**隔离**操作。

> **说明**
> - 由于资产的状态有所不同，因此在右侧的可操作按钮有所不同。资产间横向移动的欺骗事件，仅支持隔离、忽略操作。
> - 以下操作同时适用于批量处理操作。
> - 入侵事件和端口探测一般为真实攻击事件，建议封禁处理。
> - 横向移动事件一般意味着您的资产已经失陷，建议隔离处理。

- 封禁：针对危险等级较高或告警次数较多的欺骗事件，可以单击**封禁**，将该 IP 地址添加至 入侵防御 模块的封禁列表（黑名单），并选择封禁时间，添加备注，云防火墙会在时间范围内，自动拦截该 IP 地址对用户全部资产的访问。

- **放通：对于欺骗事件告警中存在重复或可能的误报，可单击放通。将该 IP 地址加入 入侵防御 模块的放通列表（白名单），并选择放通时间与放通原因，填写备注，云防火墙会在一定时间范围内，将该 IP 地址绕过入侵防御模块检测，不再拦截。如果用户不确定放通原因是否为：误报，可优先选择紧急放通，若确定为误报，可以对误报内容进行反馈，单击确定后修改即可。**

- **忽略：如果不想处理告警信息，可以单击忽略，该日志不会消失，但是在处置状态已忽略列表中可以查看记录。忽略操作不支持撤销，建议谨慎操作。**



- **隔离：单击隔离，资产实例隔离会自动下发企业安全组阻断规则，拦截选中资产的指定方向的网络访问。主要用于资产间横向移动的攻击欺骗事件，便于后续的定位排查，及时止损。**

> **说明：**
> 隔离资产实例后，支持使用运维白名单对资产进行访问，可选**手动填写 IP** 或**使用零信任防护**两种方式。
> - 仅支持手动填写10个 IP。
> - 零信任防护支持选择微信或企业微信用户允许进行资产访问，如何接入微信或企业微信用户，详情请参见 企业安全组 。

批量处置告警信息

在 攻击欺骗事件页面，支持对多条拦截信息进行处置。可以选中多条拦截信息，单击**一键拦截、放通、隔离**或**忽略**。

> **注意：**
> - 由于资产的状态不同，因此可操作按钮有所不同。隔离操作仅针对横向移动的欺骗事件，隔离失陷主机，防止影响进一步扩大。
> - 用户需要修改操作，可在**入侵防御 > 拦截列表**、**放通列表**或者**隔离列表**中恢复操作。**忽略操作不支持撤销，建议谨慎操作。**

- 超出7天告警将会失效，无法处理。

流量中心

最近更新时间：2024-05-17 15:49:31

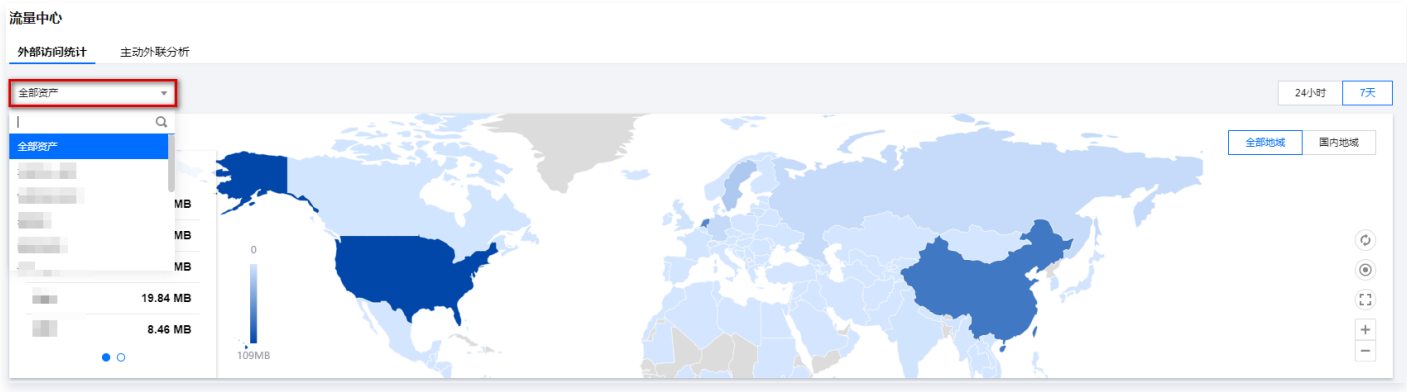
流量中心基于互联网的出向、入向流量，和 VPC 间流量的访问情况，分成外部访问统计、主动外联分析、VPC 间活动三个页面。本文档将指导您如何在流量中心模块，查看这三个页面的流量情况，解读可视化信息。

外部访问统计

用户可以在外部访问统计页面，查看入向流量的具体 IP、访问次数及流量大小等信息，同时可以在地图上筛选出具体地域对特定资产在不同时间段的访问情况，查看不同地域流量的排名。

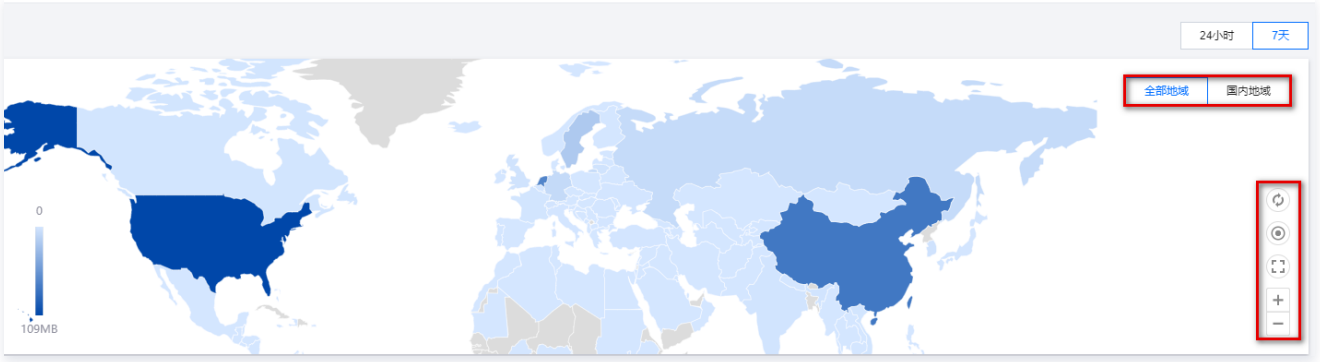
操作步骤

1. 登录 云防火墙控制台，在左侧导航栏中，单击**流量中心**，进入“外部访问统计”页签中。
2. 在“外部访问情况”模块，您可单击**全部资产**，查看具体资产在当前地域的访问情况，同时可查看不同时间段（近24小时或近7天）的流量访问情况。



3. 在地图中查看世界和中国两个地域范围内的外部流量对资产的访问情况。
   - 选择全部地域，可查看全球各国流量访问情况的分布。
   - 选择国内地域，可查看中国各省流量访问情况的分布。

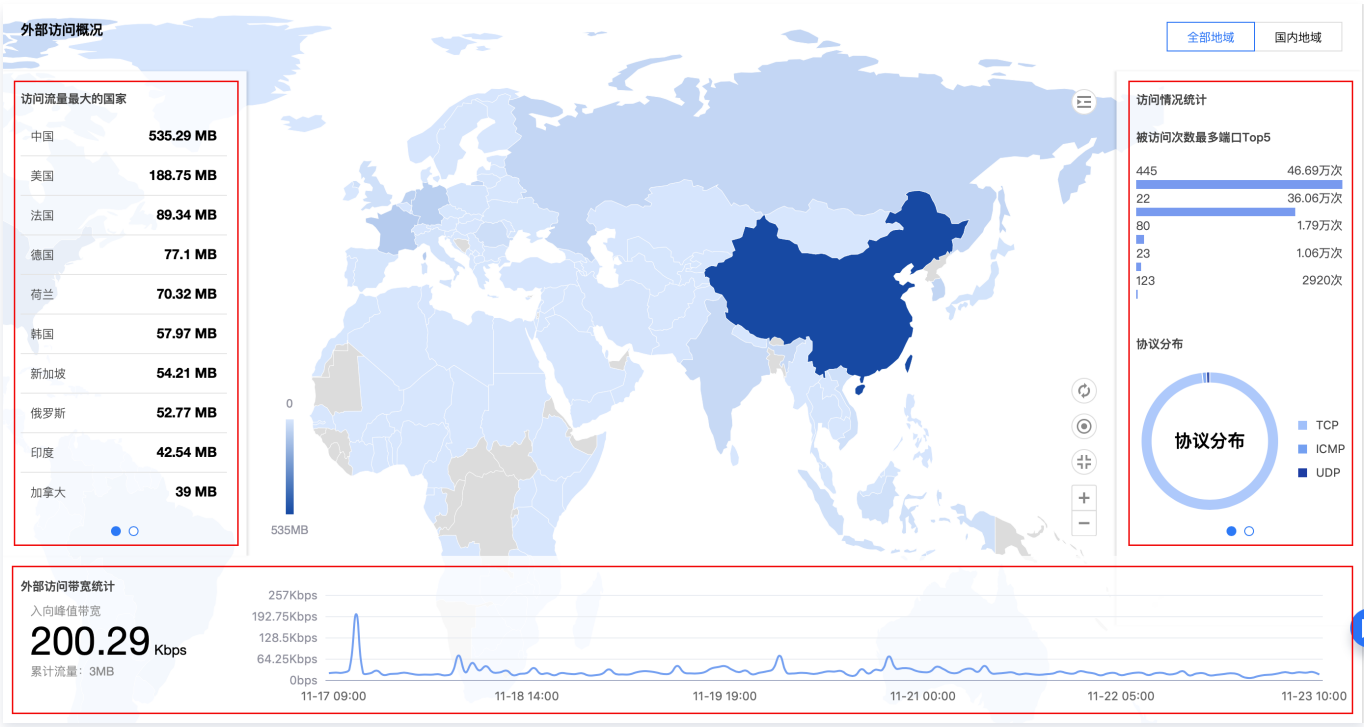
> **注意：**
> - 左侧轮播框根据访问流量大小和访问次数多少，筛选出排名前五的国家/省份，同时可以将鼠标移动至上方，查看具体 IP 访问情况。
> - 地图上的颜色深浅代表各个地域的流量访问大小（颜色越深流量访问越大），同时可以将鼠标移动至具体省份/国家上方，查看具体信息。
> - 右侧的功能按钮分别对应的功能为：刷新轮播框内的数据、重新定位地图至初始位置、展开地图、放大缩小地图。



4. 在地图右侧，单击 ，可以查看全局模式下流量访问情况。
5. 全局模式下，查看不同维度下的排名。
   - 地图左侧轮播框，根据访问流量大小和访问次数多少，筛选出排名前10的国家/省份。
   - 地图右侧轮播框，可查看被访问次数最多的端口 TOP5、外部访问的协议分布、被访问次数最多的资产 TOP5 及被访问流量最大的资产 TOP5。

> **说明：**
> 选中某特定资产后，右侧轮播框将不会展示资产排名。

- 地图下方的折线统计图，可查看当前时间范围内外部访问的流量带宽速率，并支持查看入向峰值带宽以及7天内或24小时内总流量大小。



6. 在页面下方查看外部访问 IP 列表的具体访问 IP 信息。

> **说明：**
> 由于流量信息较多，列表仅默认展示 TOP500 的 IP 访问情况。

以“互联网访问”的“外部访问”列表为例，对列表相关功能进行介绍，其他列表的功能使用方式与其相同。

6.1 在“外部访问”列表的“外部地址”搜索栏中，输入访问源**精确** IP 地址、在“目的端口”的搜索框中，输入资产**精确** IP 地址、或在“地理位置”搜索栏，输入**精确或模糊**地名，然后单击**开始搜索**，查询流量相关访问情况。

6.2 查看数据详情。您可以在访问列表中，查看流量日志、威胁画像或资产详情。

- 查看流量日志。

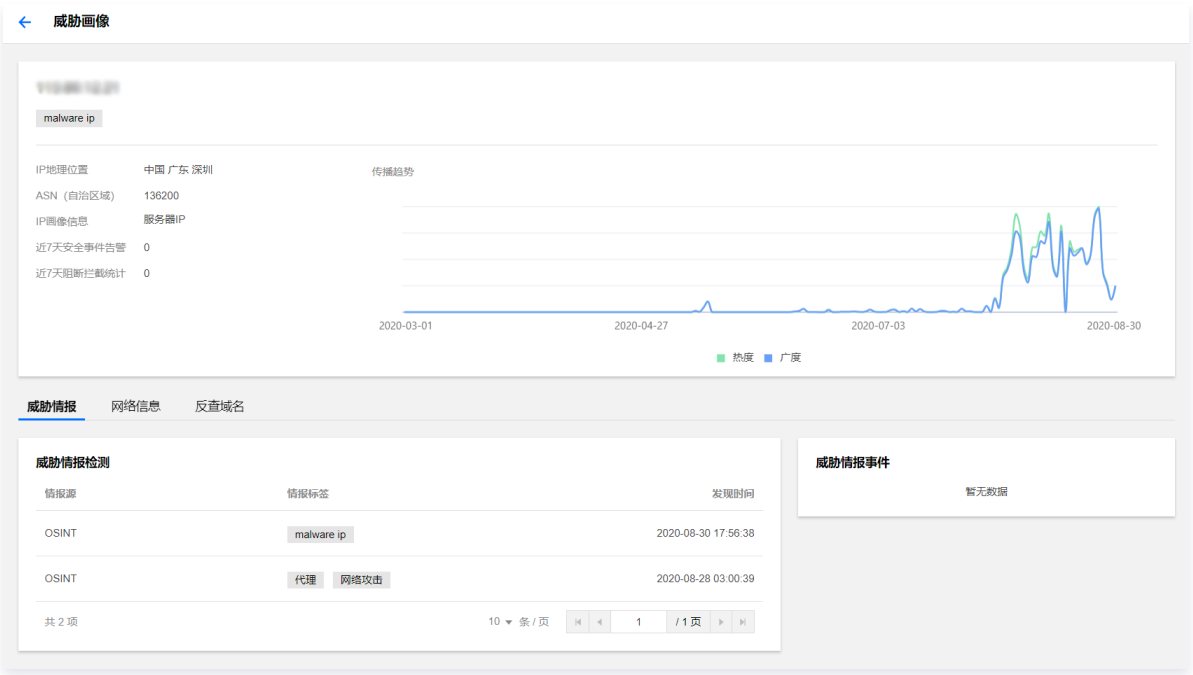
  6.2.1.1 在目标数据右侧操作栏，单击**流量日志**。

  6.2.1.2 在流量日志页面，可查看指定 IP 之间的访问详情，并以访问源和访问目的作为筛选条件，呈现同一访问源访问同一资产的具体信息。

- 查看威胁画像

  6.2.1.1 在目标数据右侧操作栏，选择**更多 > 威胁画像**。

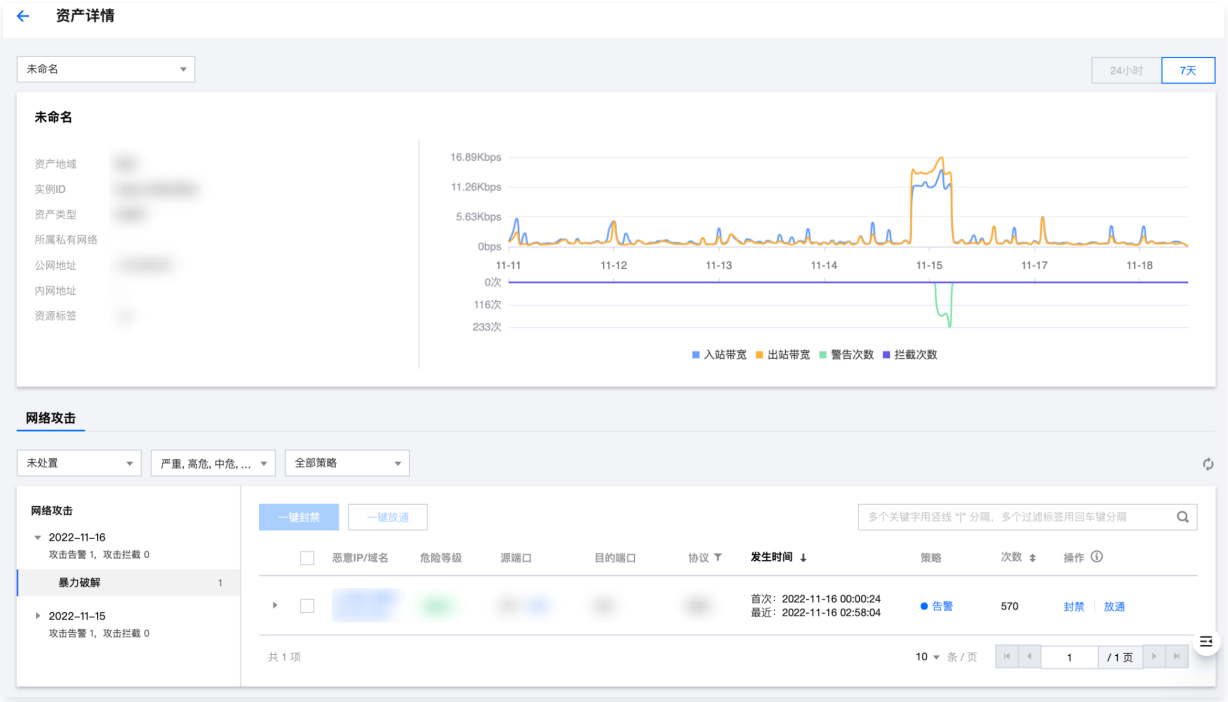
6.2.1.2 在威胁画像页面，查看该外部地址的威胁画像信息，并进一步的溯源审计。



- 查看资产详情

6.2.1.1 在目标数据右侧操作栏，选择**更多 > 资产详情**。

6.2.1.2 在资产详情页面，查看该资产的安全事件以及暴露资产等信息。



主动外联分析

您可在主动外联页面，查看近7天内资产外联详情，并可以了解具体的外联流量、外联域名及外联地址等。

操作步骤

1. 登录 云防火墙控制台，在左侧导航栏中，单击**流量中心**并进入“主动外联分析”页面。
   - 在“主动外联概况”模块，可查看“7天”或“24小时内”出向流量的访问情况，同时用户可以筛选时间和资产，来查看具体资产在某个时间段内的外部访问统计。

- 在“主动外联概况”左侧，可查看资产的外联域名、外联目的地址和外联资产的数量和告警数。用户可以通过筛选“全部资产”框，查看特定资产的外联情况。
- 可通过下方的折线图，可查看7天或24小时内的带宽速率，将鼠标悬停在折线图上，可以查看具体时间点上的带宽值。
- 在“主动外联概况”右侧，可查看7天或24小时内请求次数最多的域名 TOP5、请求次数最多的地址 TOP5、访问流量最大的地址、外联次数最多的资产 TOP5 及外联流量最大的资产 TOP5。

2. 您可以在下方的列表中，查看对应的外联流量、外联域名、外联地址和外联资产的访问情况，其中，外联域名、外联地址和外联资产均支持查看详情。

3. 以外联地址为例进行说明，其他模块查看方式相同。单击**外联地址**，在目的 IP 右侧操作栏，单击**访问详情**，进入主动外联详情页面。

4. 在主动外联详情页面，可查看资产对该 IP 近7天内或24小时内的访问次数、访问流量大小及 IP 地理位置等信息，也可以在下方列表中，查看该 IP 还访问过哪些资产。如需了解流量日志和威胁画像功能，请参见 外部访问统计 。

5. 如需进一步了解列表中某一资产的外联情况，可在实例列表右侧操作栏，单击**流量日志**或**外联详情**，可查看对应流量日志或某个特定资产在近7天或24小时内外联的 IP 和域名。

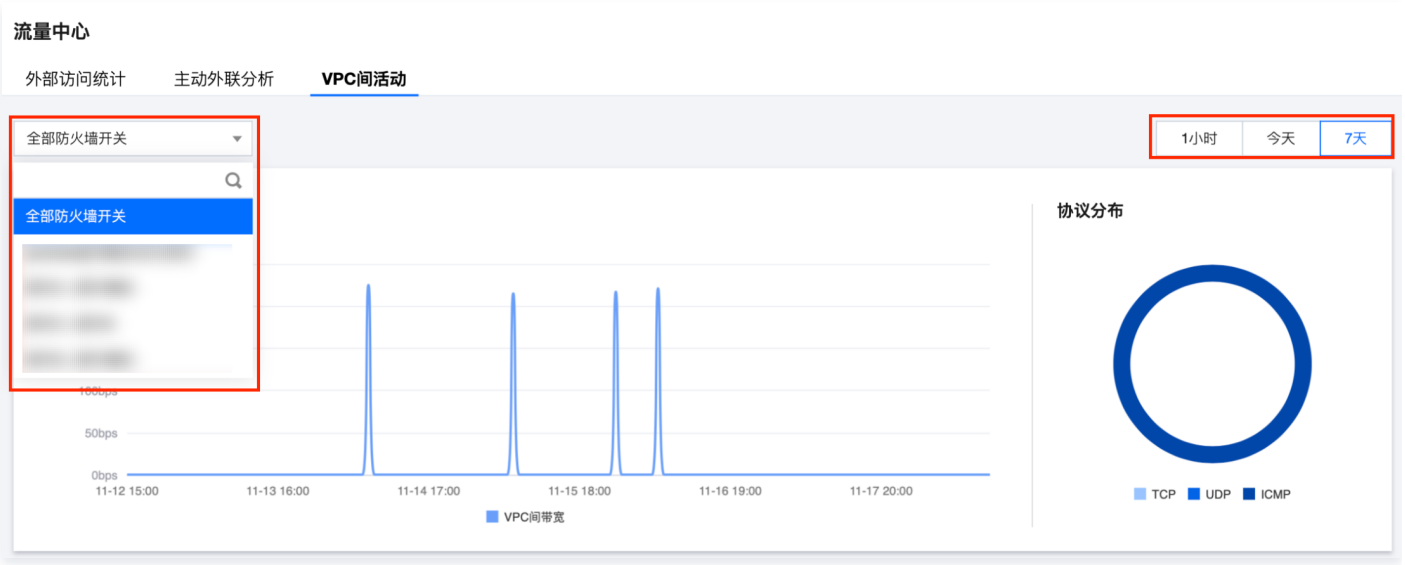
VPC 间活动

您可以在 VPC 间活动页面，查看私有云之间的流量访问情况和协议分布。

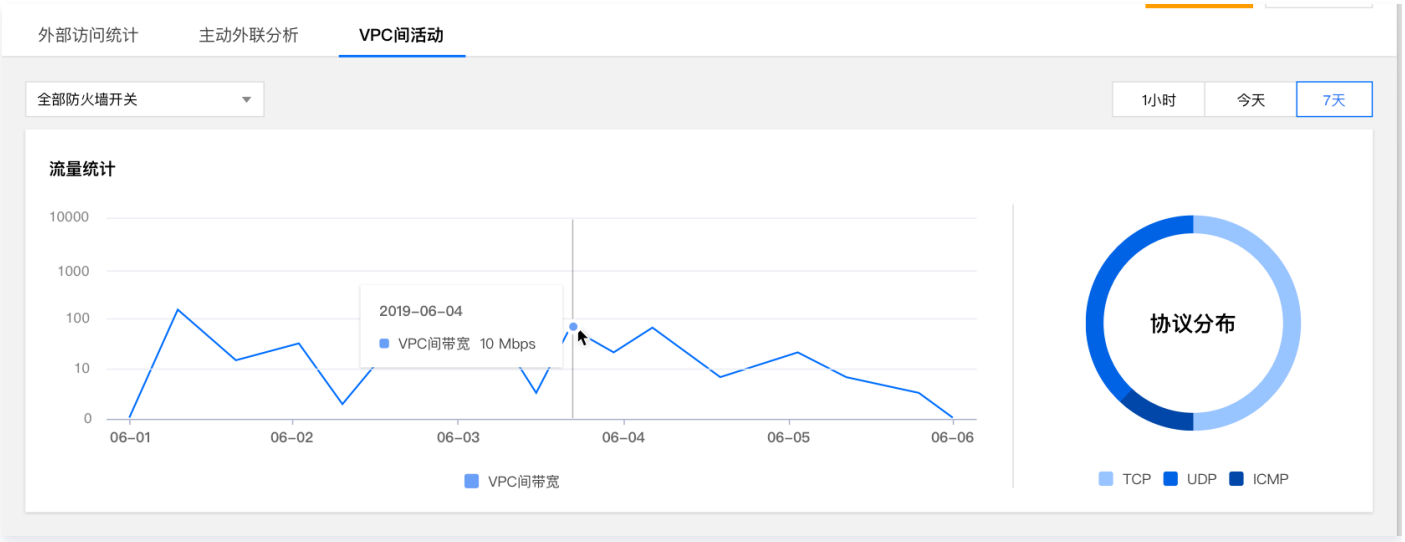
操作步骤

1. 登录 云防火墙控制台，在左侧导航栏中，单击**流量中心**并进入“VPC 间活动”页签中。

2. 在“VPC 间活动”页签的上方筛选框中，选择具体私有云的实例，并选择需要查看的时间段。



3. 将鼠标悬停在流量统计的折线图上，查看固定时间内的带宽速率，同时将鼠标悬停在右侧协议分布的扇形图上，查看具体协议的分布占比。



4. 在页面下方可查看 VPC 间具体 IP 地址，同时可查看私有云上的 IP 访问目的、访问源、访问次数等。在输入框中输入想要查询的访问源、访问目的或目的端口来进行精准搜索，详情请参见 外部访问统计 。

相关信息

如遇到流量中心相关问题，可参见 带宽相关 文档。

访问控制
规则列表配额说明

最近更新时间：2024-07-30 15:14:41

版本默认配额

当前访问控制规则包括以下几种类型：互联网边界规则、NAT 边界规则、内网间规则、企业安全组、DNS 规则。根据所购买的版本，不同版本具有的默认配额如下表所示：

版本	互联网边界规则	NAT 边界规则	内网间规则	企业安全组	DNS 规则
高级版	1000条	1000条	-	100条	-
企业版	2000条	2000条	2000条	1000条	-
旗舰版	5000条	5000条	5000条	2000条	-

占用配额统计方式

访问控制规则配额按照防火墙类型整体划分，不区分地域和方向。
列表中每条规则占用配额为1条，已占用规格数是指您对应防火墙类型下所有已添加规则数累计之和。

> **说明：**
> 例如，您 NAT 边界规则（广州）入向规则有4条，NAT 边界规则（广州）出向规则有3条，NAT 边界规则（上海）入向规则有2条，NAT 边界规则（上海）出向规则有1条；那么 NAT 边界规则配额占用数为4+3+2+1=10条。

规则展开说明

对于下发到防火墙的规则，配置的 ACL 会按照最小粒度拆分为多条规则下发至引擎，故引擎统计的规则数并非列表规则数，而是下发规则数。下发规则数的相关规格可参考 实例规格 。
规则展开公式如下：
下发规则数 = 源地址个数 × 目的地址个数 × 端口个数 × 协议个数。

> **说明：**
> - 对于源地址和目的地址，1个 IP、CIDR、IP 范围、域名/子域名均视作为1个最小展开单元。
> - 对于端口，单个端口、连续端口段、全部端口均视作为1个最小展开单元。
> - 对于协议，除 ANY 外的单个协议均视作为1个最小展开单元。
>   - 当访问源及访问目的均为 IP 时，此时为4层 ANY 协议视作1个最小展开单元。
>   - 当访问目的为域名时，此时为7层 ANY 协议视作6个最小展开单元。
> - 例如：访问源0.0.0.0/0为1个 CIDR，访问目的是一个域名地址模板包含了2个域名，目的端口80,443/446其中一个为单端口一个为端口段，协议为7层的 ANY 协议；故下发规则数=1*2*2*6=24条。

下发规则数限制

当引擎达到最大下发规则数限制后，将无法继续配置ACL规则，请合理管理规则。具体防火墙下发规则数限制如下：
- 互联网边界旁路防火墙：单租户最大支持10000条下发规则数，无法扩展，请合理优化规则。
- NAT 边界防火墙：与实例规格相关，可通过提升实例规格扩展下发规则数限制，详见 NAT 边界防火墙实例规格 。
- VPC 间边界防火墙：与实例规格相关，可通过提升实例规格扩展下发规则数限制，详见 VPC 防间火墙实例规格 。

版权所有：腾讯云计算（北京）有限责任公司

互联网边界规则

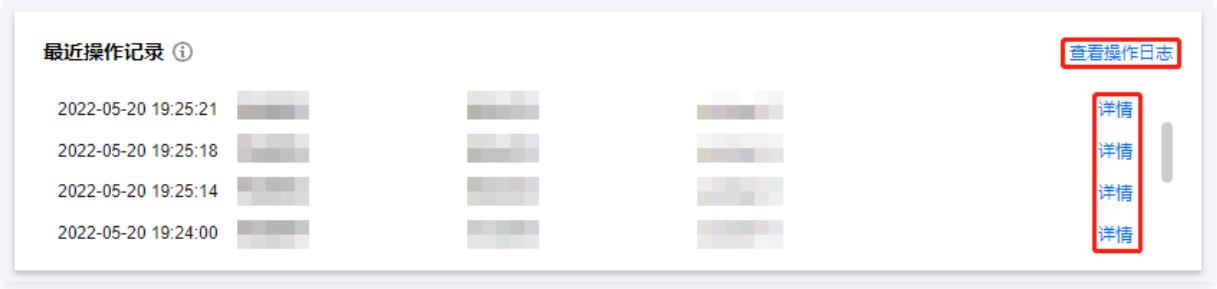
最近更新时间：2025-06-18 09:47:32

访问控制规则支持域名过滤，以及地理位置要求的流量过滤。互联网边界规则提供两张访问控制规则列表，分别是入站规则与出站规则，**入站规则**：管控外到内的南北向流量。**出站规则**：管控内到外的南北向流量。本文档将以“入站规则”为例，进行相关操作说明，“出站规则”操作同理。

操作指南

1. 登录 云防火墙控制台，在左侧导航栏中，选择**访问控制** > **互联网边界规则**。
2. 在互联网边界规则页面，单击**入站规则**，进入入站规则页面。

3. 在入站规则页面，可查看最近操作记录。最近操作记录展示了用户最近对规则列表进行的操作：
   - 单击**详情**，可查看该条操作记录详情。



   - 单击**查看操作日志**，可查看详细操作记录。

> **说明：**
> 因投递日志需1分钟左右的时间，所以最近操作记录更新会有稍许延迟。

4. 添加规则，在入站规则页面，可进行规则的配置。
   4.1 在入站规则页面，单击**添加规则**，将弹出“添加入站规则”的弹窗。
   4.2 在“添加入站规则”的弹窗中，可进行规则的配置。访问源类型可选 IP 地址、地理位置、云厂商和 地址模板，访问目的类型可选 IP 地址、资产实例、资源标签、地址模板和资产分组，并根据规则重要性勾选执行顺序，完成源目的类型和顺序的选择后，填写访问源、访问目的、目的端口、协议、策略以及描述等信息，单击**确定**完成配置。

> **注意**
> - 入站规则：访问源填写0.0.0.0/0时，后台会自动关联全部公网 IP，填写 CIDR 地址同理，仅对该网段内的公网 IP 生效。
> - 出站规则：与入站规则相同。

- **字段说明：**
  - **访问源的类型：**
    - IP 地址：任意 IP 地址或 CIDR 格式地址例如10.10.10.10或10.10.10.10/24。支持多个对象使用逗号分隔。
    - 地理位置：为 IP 对应的实际地理位置，包含中国大陆地区各个省、中国港澳台地区及海外的各个州。

      > **说明**
      > 仅企业版和旗舰版云防火墙支持地理位置功能，如需使用该功能，可以升级为 企业版或旗舰版 云防火墙。

    - 云厂商：为各个云服务厂商品牌对应的服务 IP。
    - 地址模板：为用户自定义设置的 IP 地址模板。
  - **访问目的类型：**
    - IP 地址：入站规则的访问目的仅对您的公网 IP 生效，若填写 CIDR 地址，则后台会自动关联为该地址段内包含的您的全部公网 IP。支持多个对象使用逗号分隔。
    - 资产实例：入站方向选择具体实例为访问目的。
    - 资源标签：根据资源的标签来选择访问目的，标签内实例的公网 IP 会匹配互联网边界规则。
    - 地址模板：选择用户自定义设置的 IP 地址模板为访问目的。
    - 资产分组：选择用户自定义设置的资产分组为访问目的。
  - **规则优先级**：定义规则执行的优先级，最先执行或最后执行。
  - **执行顺序**：访问控制规则的执行顺序，出站规则和入站规则的执行顺序互不影响，执行顺序较高的规则被优先匹配，命中某条规则后，不再匹配后序规则。当您修改某条规则的执行顺序时，原本该位置的规则的执行顺序+1，以此类推。当您删除某条规则时，后序所有规则的执行顺序-1。
  - **访问源**：入站规则访问源可以设置任意的 IP/CIDR 格式地址，同时也支持地理位置、云厂商和地址模板等参数。
  - **访问目的**：入站规则的访问目的仅对公网 IP 生效，同时还支持资产实例、资源标签、地址模板和资产分组等参数。如果是出站规则，访问源和访问目的的参数对调。
  - **目的端口**：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。例如“80”、“80/80”、“-1/-1”、“1/65535”或“80,443,3380/3389”
  - **协议**：串行防火墙支持的协议：TCP、UDP、ICMP、HTTP、HTTPS、HTTP/HTTPS、SMTP、SMTPS、SMTP/SMTPS、TLS/SSL、DNS 以及 FTP；旁路防火墙支持的协议：TCP、HTTP/HTTPS（仅出向支持）、TLS/SSL（仅出向支持）。
  - **策略**：
    - 放行：放通命中规则的流量，记录命中次数但不记录访问控制日志，且记录流量日志。
    - 观察：放通命中规则的流量，记录命中次数并记录访问控制日志与流量日志。
    - 阻断：拦截命中规则的流量，记录命中次数并记录访问控制日志，流量日志记录流量的一个请求数据包信息。
  - **生效范围**：当前规则生效的防火墙范围，可选“全局规则”、“串行防火墙”或“旁路防火墙”。
  - **描述**：用于描述规则，最多支持50个字符。
- **互联网边界通配规则：**

输入字段	输入示例	说明
访问源/访问目的	0.0.0.0/0	表示全部 IP。
域名（仅出站规则中）	*	表示全部域名。
域名（仅出站规则中）	*.aa.com	表示以*开头的二级域名：aa.com。

目的端口	-1/-1	表示全部端口。
目的端口	1/65535	表示全部端口。
目的端口	80,443,3389	表示对80、443、3389三个端口生效。
目的端口	80/443	表示对80到443之间的全部端口生效。
目的端口	80/443,3389	表示对80到443之间全部端口与3389端口生效。

说明：

- 输入域名的操作如下：在 访问控制 > **互联网边界规则** > **出站规则**页面，单击**添加规则**，选择访问目的，根据出站规则，输入所需域名，单击**确定**保存。
- 出站规则：访问目的支持任意 IP 地址、CIDR 地址和域名，支持 * 开头的通配符域名以及 * 表示的全部域名。

5. 在右侧操作栏单击**复制**，添加多条规则。

说明

在“添加入站规则”的弹窗中，一行代表一条规则，每次添加规则默认插入到列表的最后位置，即执行顺序最大，优先级最低的位置。

- **场景1**：已在本地完成规则列表的编辑，需要批量添加规则提升效率。

  5.1.1 在右侧操作栏单击**复制**，可在当前位置的下方新增一行规则，单次最多支持添加10条规则。

  5.1.2 完善表单中所有字段。

  5.1.3 提交前，检查批量添加规则的执行顺序是否符合预期。

  5.1.4 单击**确定**，提交所配置的规则。

- **场景2**：需要同时对某个 IP 配置多条规则。

  5.1.1 首先编辑一行规则，只编辑需要重复填写的部分。

  5.1.2 在右侧操作栏单击**复制**，可在当前位置的下方新增一行规则，并自动复制上一行已经填写的内容，单次最多支持添加10条规则。

5.1.3 完善表单中其他字段，补充不需要重复填写的部分。

5.1.4 提交前，检查批量添加规则的执行顺序是否符合预期。

5.1.5 单击**确定**，提交所配置的规则。

6. 规则添加完成后，即可在规则列表中查看相关规则。
7. 导入规则，单击**导入规则**，可以从本地选择文件导入，您可以指定导入位置、下载导入模板和导出现有规则。

8. 规则备份与回滚，请参见 规则备份 文档。

相关信息

- 如需在云防火墙控制台对 NAT 边界的入向与出向流量进行管控，请参见 NAT 边界规则 。
- 如需在云防火墙控制台设置内网间规则，请参见 内网间规则 。
- 如需了解云防火墙的访问控制功能的特殊应用场景，请参见 特殊应用场景 。
- 如遇到互联网边界规则相关问题，请参见 互联网边界防火墙 文档。

版权所有：腾讯云计算（北京）有限责任公司

NAT 边界规则

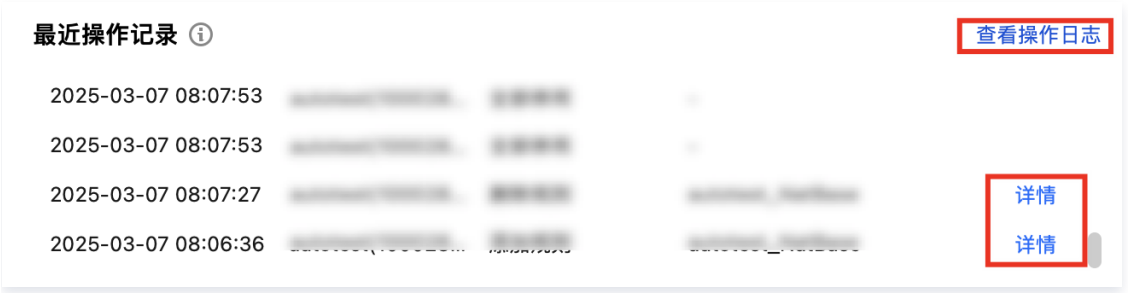
最近更新时间：2025-06-30 10:49:21

访问控制规则支持域名过滤，以及地理位置要求的流量过滤。NAT 边界规则提供两张访问控制规则列表，分别是入向规则与出向规则，**入向规则**：在互联网边界内，管控由外到内的南北向流量。**出向规则**：在互联网边界内，管控由内到外的南北向流量。本文档将以“入向规则”为例，进行相关操作说明，“出向规则”操作同理。

操作指南

1. 登录 云防火墙控制台，在左侧导航栏中，选择**访问控制** > **NAT 边界规则**。
2. 在 NAT 边界规则界面，单击**入向规则**，进入入向规则界面。

3. 在入向规则界面，可选择不同地域来创建访问控制规则，以及查看规则列表（入向规则、出向规则已使用的额度以及规则列表总的配额）、最近操作记录和访问控制规则详情。最近操作记录展示了用户最近对规则列表进行的操作：
   - 单击**详情**可查看该条操作记录详情。
   - 单击**查看操作日志**，可查看详细操作记录。



4. 添加规则，在入向规则页面，可进行规则的配置，以添加入向规则为例进行说明。
   4.1 在入向规则页面，单击**添加规则**，将弹出“添加入向规则”的弹窗。
   4.2 在“添加入向规则”的弹窗中，可进行规则的配置。访问源类型可选 IP 地址、地理位置、云厂商及 地址模板，访问目的类型可选 IP 地址、资产实例、资源标签、地址模板及资产分组，并根据规则重要性来勾选最先或者最后执行。填写好访问源和访问目的之后，再填写目的端口，选择对应的协议和要执行的策略等信息，并在描述一栏做好备注，单击**确定**，即可完成规则的配置。

> **说明：**
> - 访问目的区域： 指云上实例所在的地域
> - 访问源的类型：添加入向规则时， 指外部访问源的类型。

字段说明：

- **访问源的类型：**
  - IP 地址：任意 IP 地址或 CIDR 格式地址例如10.10.10.10或10.10.10.10/24。支持多个对象使用逗号分隔。
  - 地理位置：为 IP 对应的实际地理位置，包含中国大陆地区各个省、中国港澳台地区及境外的各个州。

    > **说明**
    > 仅企业版和旗舰版云防火墙支持地理位置功能，如需使用该功能，可以升级为 企业版或旗舰版 云防火墙。

  - 云厂商：为各个云服务厂商品牌对应的服务 IP。
  - 地址模板：为用户自定义设置的 IP 地址模板。
- **访问目的类型：**
  - IP 地址：入向规则的访问目的仅对您的公网 IP 生效，若填写 CIDR 地址，则后台会自动关联为该地址段内包含的您的全部公网 IP。支持多个对象使用逗号分隔。
  - 资产实例：入向规则选择具体实例为访问目的。
  - 资源标签：根据资源的标签来选择访问目的，标签内实例的公网 IP 会匹配互联网边界规则。
  - 地址模板：选择用户自定义设置的 IP 地址模板为访问目的。
  - 资产分组：选择用户自定义设置的资产分组为访问目的。
- **端口协议类型：**定义访问目的端口的输入方式。旁路防火墙仅支持手动填写端口。
- **规则优先级：**定义规则执行的优先级，最先执行或最后执行。
- **执行顺序：**访问控制规则的执行顺序，出向规则和入向规则的执行顺序互不影响，执行顺序较高的规则被优先匹配，命中某条规则后，不再匹配后续规则。当您修改某条规则的执行顺序时，原本该位置的规则的执行顺序+1，以此类推。当您删除某条规则时，后序所有规则的执行顺序-1。
- **访问源：**入向规则访问源对所有公网 IP 生效，支持 IP 地址、地理位置、云厂商和地址模板。
- **访问目的：**入向规则访问目的仅对当前地域内的所有内网资产生效，支持 IP 地址、资产实例、资源标签、地址模板和资产分组，出向规则访问源和访问目的支持的类型正好相反。
- **域名规则（出向规则支持）：**根据访问中请求的域名，判断是否放行，不校验域名解析的 IP。
- **域名解析规则（出向规则支持）：**根据协议、实例所在的地域，放行域名实际请求的 IP。
- **目的端口：**TCP/UDP 规则支持单端口号、基于'/'的端口段以及英文逗号分隔的离散端口值，例如“80”、“80/80”、“-1/-1”、“1/65535”或“80,443,3380/3389”，ICMP 规则不需要配置端口。
- **协议：**当前版本的入向规则支持 TCP和UDP协议；出向规则支持 TCP、UDP、ICMP、HTTP、HTTPS、SMTP、SMTPS、DNS 和 FTP 等协议。
- **策略说明：**
  - 放行：放通命中规则的流量，记录命中次数但不记录访问控制日志，且记录流量日志。
  - 观察：放通命中规则的流量，记录命中次数并记录访问控制日志与流量日志。
  - 阻断：拦截命中规则的流量，记录命中次数并记录访问控制日志，流量日志记录流量的一个请求数据包信息。
- **生效范围：**当前规则生效的防火墙范围，可选“全局规则”、指定地域实例生效或指定防火墙实例生效。
- **描述：**用于描述规则，最多支持50个字符，支持通过##的方式插入规则的特殊设置，当前版本支持的设定有#长连接#，适用于有长连接业务场景。
- **NAT 边界通配规则：**

  防火墙提供了不同的通配 IP、通配端口和通配域名的规则：

输入字段	输入示例	说明

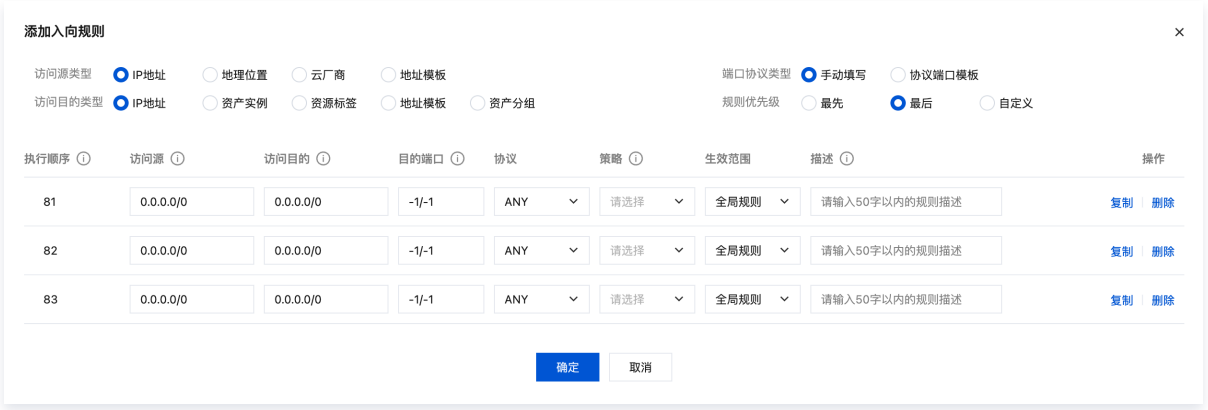
访问源/访问目的	0.0.0.0/0	表示全部 IP。
域名	*	表示全部域名。
域名	*.aa.com	表示以*开头的二级域名：aa.com。
目的端口	-1/-1	表示全部端口。
目的端口	1/65535	表示全部端口。
目的端口	80,443,3389	表示对80、443、3389三个端口生效。
目的端口	80/443	表示对80到443之间的全部端口生效。
目的端口	80/443,3389	表示对80到443之间全部端口与3389端口生效。

5. 在右侧操作栏单击**复制**，添加多条规则。

> **说明：**
> 在“添加入向规则”的弹窗中，一行代表一条规则，每次添加规则默认插入到列表的最后位置，即执行顺序最大，优先级最低的位置。

- **场景1**：已在本地完成规则列表的编辑，需要批量添加规则提升效率。

  5.1.1 在右侧操作栏单击**复制**，可在当前位置的下方新增一行规则，单次最多支持添加10条规则。



  5.1.2 完善表单中所有字段。

  5.1.3 提交前，检查批量添加规则的执行顺序是否符合预期。

  5.1.4 单击**确定**，提交所配置的规则。

- **场景2**：需要同时对某个 IP 配置多条规则。

  5.1.1 首先编辑一行规则，只编辑需要重复填写的部分。

  5.1.2 在右侧操作栏单击**复制**，可在当前位置的下方新增一行规则，并自动复制上一行已经填写的内容，单次最多支持添加10条规则。

  5.1.3 完善表单中其他字段，补充不需要重复填写的部分。

  5.1.4 提交前，检查批量添加规则的执行顺序是否符合预期。

  5.1.5 单击**确定**，提交所配置的规则。

6. 导入规则，单击**导入规则**，可以从本地选择文件导入，您可以指定导入位置和下载导入模板。

7. 规则备份与回滚，请参见 规则备份 文档。

相关信息

- 如需在云防火墙控制台对互联网边界的入向与出向流量进行管控，请参见 互联网边界规则 。
- 如需在云防火墙控制台设置内网间规则，请参见 内网间规则 。
- 如需了解云防火墙的访问控制功能的特殊应用场景，请参见 特殊应用场景 。
- 如遇到 NAT 边界规则相关问题，可参见 NAT 边界防火墙 。

内网间规则

最近更新时间：2025-04-17 15:08:22

内网间规则提供一个访问控制列表，创建规则时对规则生效范围进行配置，从而支持对不同 VPC 间的流量互通提供访问控制。本文将介绍如何在云防火墙控制台设置内网间规则。

添加规则

1. 登录 云防火墙控制台，在左侧导航栏中，选择**访问控制** > **内网间规则**。

> **说明**
> - 区别于互联网边界和 NAT 边界访问控制列表，内网间访问控制列表不区分方向区。
> - 本端 VPC 与对端 VPC 是等价的，在配置规则时，可以根据访问源与访问目的所在的 CIDR 网段判断所属 VPC，进而区分方向。

2. 在内网间规则页面，单击**添加规则**，进入添加规则页面。
3. 在添加规则页面，填写访问源 IP、访问目的 IP 、目的端口、协议、策略、生效范围等信息，单击**确定**完成规则配置。

字段说明：

- **执行顺序**：访问控制规则的执行顺序，与防火墙开关中对应规则列表的执行顺序互不影响，执行顺序较高的规则会被优先匹配，命中某条规则后，则不再继续匹配后序规则。当您修改某条规则的执行顺序时，原本该位置规则的执行顺序+1，以此类推。当您删除某条规则时，后序所有规则的执行顺序-1。
- **访问源**：支持0.0.0.0/0作为通配规则的访问源（仅生效于所选生效范围之间），除此之外访问源只能填写本端/对端VPC的CIDR中的IP或子网段，且不与访问目的在同一个VPC网段内。单击**详情**，可查看内网间规则关联的访问源网络实例详情。
- **访问目的**：支持0.0.0.0/0作为通配规则的访问目的（仅生效于所选生效范围之间），除此之外访问目的只能填写本端或对端 VPC 的 CIDR 中的 IP 或子网段，且不与访问源在同一个 VPC 网段内。单击**详情**，可查看内网间规则关联的访问目的网络实例详情。
- **目的端口**：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。例如“80”、“80/80”、“-1/-1”、“1/65535”或“80,443,3380/3389”。
- **协议**：支持 TCP、UDP、ICMP、HTTP、HTTPS、SMTP、SMTPS、DNS 和 FTP 等协议。
- **策略说明**：
  - 放行：放通命中规则的流量，记录命中次数但不记录访问控制日志，且记录流量日志。
  - 观察：放通命中规则的流量，记录命中次数并记录访问控制日志与流量日志。
  - 阻断：拦截命中规则的流量，记录命中次数并记录访问控制日志，流量日志记录流量的一个请求数据包信息。
- **生效范围**：
  - 全局策略：规则对所有 VPC 间防火墙管控的流量都生效。
  - 选定一个 VPC 间防火墙开关：规则仅对该防火墙开关管控的内网间流量生效。
- **描述**：用于描述规则，最多支持50个字符，支持通过##的方式插入规则的特殊设置，当前版本支持的设定有#长连接#，适用于长连接业务场景。
- **VPC 间通配规则**：支持通配的 IP 地址段，详情可参见 互联网边界规则 中的互联网边界通配规则。

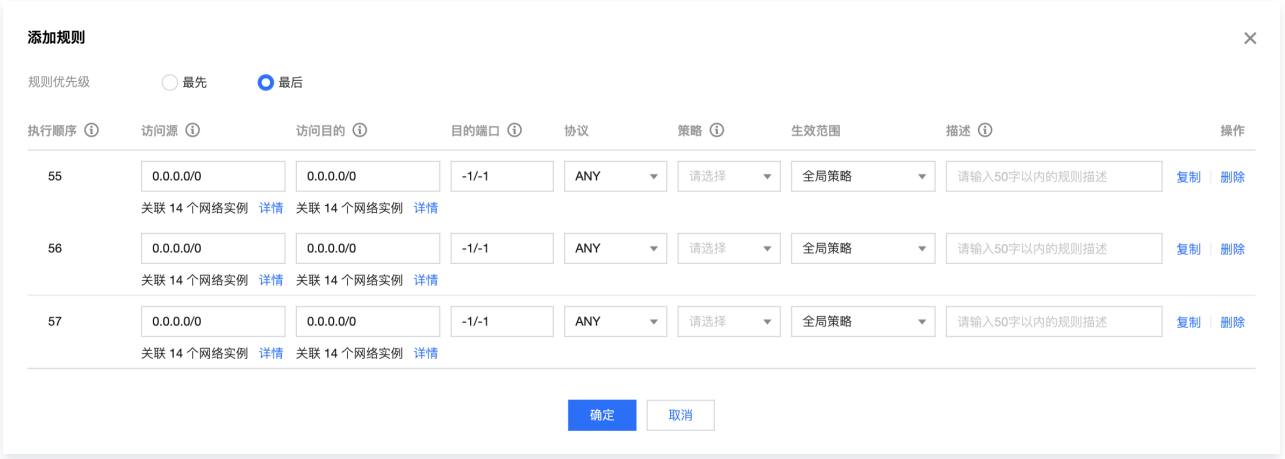
> **注意**
> - VPC 间防火墙对应的本端 VPC 与对端 VPC 的 CIDR 网段不能相同，也不能重叠，否则将无法开启防火墙开关。
> - 内网间访问控制规则中，访问源与访问目的仅支持填写：本端/对端 VPC 的 CIDR 地址中的 IP 地址或 CIDR 子网段，由于本端 VPC 和对端 VPC 的 CIDR 不能相同，通过“访问源”、“访问目的”便可以区分规则所控制的流量方向。
> - 若填写本端 VPC 或对端 VPC 的 CIDR 以外的地址，则规则无法生效。

- 当“访问源”和“访问目的”填写0.0.0.0/0时，可以用来表示 VPC 的全部地址。

4. 在右侧操作栏单击**复制**，添加多条规则。

说明
在“添加入站规则”的弹窗中，一行代表一条规则，每次添加规则默认插入到列表的最后位置，即执行顺序最大，优先级最低的位置。

- **场景1**：已在本地完成规则列表的编辑，需要批量添加规则提升效率。
  4.1.1 在右侧操作栏单击**复制**，可在当前位置的下方新增一行规则，单次最多支持添加10条规则。



  4.1.2 完善表单中所有字段。
  4.1.3 提交前，检查批量添加规则的执行顺序是否符合预期。
  4.1.4 单击**确定**，提交所配置的规则。
- **场景2**：需要同时对某个 IP 配置多条规则。
  4.1.1 首先编辑一行规则，只编辑需要重复填写的部分。
  4.1.2 在右侧操作栏单击**复制**，可在当前位置的下方新增一行规则，并自动复制上一行已经填写的内容，单次最多支持添加10条规则。

  4.1.3 完善表单中其他字段，补充不需要重复填写的部分。
  4.1.4 提交前，检查批量添加规则的执行顺序是否符合预期。
  4.1.5 单击**确定**，提交所配置的规则。

5. 规则添加完成后，即可在规则列表中查看相关规则。

导入规则

在内网间规则页面，单击**导入规则**，可以从本地选择文件导入，您可以指定导入位置、下载导入模板和导出现有规则。

规则备份与回滚

规则备份与回滚，请参见 规则备份 文档。

> **注意**
> 改版前已经备份过的内网间规则不支持回滚，如有需要请 提交工单 联系我们。

相关信息

- 如需在云防火墙控制台对互联网边界的入向与出向流量进行管控，请参见 互联网边界规则 。
- 如需在云防火墙控制台对 NAT 边界的入向与出向流量进行管控，请参见 NAT 边界规则 。
- 如需了解云防火墙的访问控制功能的特殊应用场景，请参见 特殊应用场景 。
- 如遇到 VPC 间规则相关问题，可参见 VPC 间防火墙 文档。

版权所有：腾讯云计算（北京）有限责任公司

企业安全组
功能简介

最近更新时间：2024-05-17 15:49:31

企业安全组是一种全新的安全组控制平面，可以取代云服务器控制台的安全组管理界面。对安全组的配置逻辑进行了重新设计，维护了统一的访问控制管理页面，极大优化了安全组的使用体验。云防火墙提供基于五元组的规则配置界面，并通过智能转换算法自动下发安全组策略，大幅简化了安全组的配置操作。

说明：
云防火墙已推出新版企业安全组，新版企业安全组是在旧版的基础上做了一些改进，主要在配置项、逻辑等方面做了优化，规则匹配条件更加精细化，策略更加直观，便于理解和管理。推荐您可以使用 新版企业安全组，关于新旧版具体差异可以参见 热点问题。

企业安全组特点

- 大幅简化了安全组的配置操作，并保留五元组规则的使用习惯。
- 更加方便的支持 VPC 间、子网间及专线接入的访问控制。
- 提供安全组的访问控制日志，方便回溯阻断情况和日常排障。
- 无需改变网络架构，对网络稳定性没有任何影响，在网络性能方面也不产生额外的瓶颈。

企业安全组限制

企业安全组基于云服务器安全组的底层架构进行开发，所以受限于安全组的底层功能实现和资源配额。

企业安全组规则

规则的组成部分

- 访问源和访问目的：根据入站或出站的方向不同，可以是 IP 地址、CIDR 地址块、实例、子网或私有网络。
- 目的端口：目的端口号。当协议类型为 ICMP 或 ANY 时，此项无需配置。
- 协议类型：目前支持 TCP、UDP 和 ICMP。ANY 代表全部已支持的协议。
- 策略：规则命中后，所执行的操作。
  - 放行策略，放行命中规则的流量，不记录访问控制日志。
  - 阻断策略，拦截命中规则的流量，记录访问控制日志。

规则的优先级

安全组规则具有优先级，规则优先级通过规则在列表中的位置来表示，列表顶端规则优先级最高，列表底端规则优先级最低。
执行顺序是从高优先级向低优先级进行逐条匹配，规则命中后，则不再匹配后续规则。
入站规则和出站规则，分属不同的规则列表，优先级互不影响。
如需使用企业安全组功能，请参见 配置步骤。

自动双向下发

为了提高安全组的配置效率，企业安全组提供了“自动双向下发”功能。在内网对内网的双向阻断或放行的场景中，不再需要在两个方向配置两条一模一样的规则。使用这个功能可以自动实现这种操作，降低规则配置的工作量。

版权所有：腾讯云计算（北京）有限责任公司

当访问源地址填写为实例、子网或私有网络地址时，可通过“自动双向下发”功能，自动配置一条相同的出站规则（执行顺序为最高）。

> **注意**
> 只适用于内网到内网的通信场景。

例如，假设有两个实例，实例1的 IP 为 IP1，实例2的 IP 为 IP2。
用户对实例1和实例2分别配置了 deny all 的安全组，此时想要对实例1到实例2的访问做单向放行，需要手动配置两条安全组规则：

- 实例1，出站方向对 IP2 放行。
- 实例2，入站方向对 IP1 放行。

使用“自动双向下发”功能，只需要手动配置其中的一条规则，另一条，由企业安全组自动生成，详情请参见 实例间单向访问的自动双向下发 进行操作。

日志

安全组阻断日志

安全组阻断日志 可展示所有企业安全组阻断策略生效的情况，目前仅支持 少量机型 。

企业安全组操作日志

企业安全组操作日志 用于记录某个账号在企业安全组页面中进行的操作。

配置步骤

最近更新时间：2024-05-17 15:49:31

本文将为您介绍如何通过企业安全组进行配额管理及添加规则等操作。

> **说明：**
> 云防火墙已推出新版企业安全组，新版企业安全组是在旧版的基础上做了一些改进，主要在配置项、逻辑等方面做了优化，规则匹配条件更加精细化，策略更加直观，便于理解和管理。推荐您可以使用 新版企业安全组，关于新旧版具体差异可以参见 热点问题。

前提条件

- 需已将云防火墙 升级到企业版或旗舰版。
- 首次使用企业安全组，需要已进行 CAM 授权。在您开通企业安全组后，首次进入**访问控制** > 企业安全组 **页面或访问控制日志** > **企业安全组** 页面时，请按照提示进行授权操作。

  > **说明：**
  > 日志投递功能需要对云防火墙服务角色 CFW_QcsRole，关联策略 QcloudAccessForCFWRoleIn EnterpriseSecurityGroup 、QcloudAccessForCFWRoleInLogService 权限。

- 开通 CLS（日志服务）。当您完成 CAM 授权后，网络流日志会投递到您的腾讯云 CLS（日志服务）中。若您尚未开通此功能，请按照控制台提示，手动开启。开启 CLS 后，即可在刷新云防火墙的**访问控制日志** > 企业安全组 页面，查看相关日志内容。

操作步骤

步骤1：配额管理

企业安全组会占用您的安全组配额，您可以在企业安全组页面查看并管理相关安全组配额。

1. 登录 云防火墙控制台，在左侧导航中，选择**访问控制** > **企业安全组**。
2. 在企业安全组页面的规则列表概况右上角，单击**配额详情**，可以查看安全组配额。

3. 在安全组配额详情页面，可查看各地域的安全组配额详情，并根据需求查看各关联实例及安全组详情。

字段说明：

- **已有安全组数**：已配置的安全组个数。
- **安全组数配额**：每个地域允许创建的安全组数上限。
- **安全组规则数**：每个安全组允许的出站或入站规则数。
- **安全组绑定实例数**：单个安全组关联的云服务器实例数。
- **实例绑定安全组数**：每个实例可以关联的安全组个数。
- **关联实例**：已关联实例列表，并可查看各实例详情。
- **安全组列表**：已有安全组列表，并可查看各安全组详情。

4. （可选）安全组的配额是有限的，当您完成一次添加规则、插入规则或编辑规则的操作后，若安全组配额不足，系统会提示您调整相应的安全组配额，在企业安全组页面的规则列表概况右上角，单击**管理配额**，去工单系统中申请安全的相关配额即可。

步骤2：添加规则

规则分为入站规则和出站规则，规则列表在同一时间只允许一个用户进行操作，本文将以入站规则为例进行说明（出站规则同理）。

1. 在 企业安全组页面，左上角选择需要操作的地域。

> **说明：**
> 每个地域都有独立的企业安全组的入站规则列表和出站规则列表。

2. 在企业安全组页面下方，选择**入站规则>添加规则**。
3. 在添加入站规则的弹窗中，填写相关字段，单击**确定**。
   - 规则优先级：“最先”是将新规则插入到规则列表的最前方，优先级最高。“最后”是将新规则插入到规则列表的最后，优先级最低。
   - 访问目的类型：包括“云服务器”、“云数据库”、“弹性网卡”及“负责均衡”，并根据不同访问目的类型，填写相关字段。
   - 自动双向下发：当访问源地址填写为实例、子网、私有网络地址时，可通过自动双向下发，分配一条相同的出站规则（执行顺序为最高），适用于内网对内网的双向放行的场景。

> **注意：**
> - 当资产绑定唯一安全组时，安全组默认阻断全部。
> - 若您的资产中存在没有绑定任何安全组的资产实例，下发企业安全组策略会为这些资产绑定唯一安全组，存在较高安全风险，请谨慎操作。

4. 添加完成，该入站规则将出现在入站规则列表中。

5. 添加完入站规则后，在私有网络控制台的 安全组页面 中，可查看企业安全组自动生成的安全组，自动配置了安全组规则和关联实例。

> **注意**
> 请您不要在其他位置手动修改云防火墙维护的安全组或路由表（如 NAT 路由表、CVM 安全组等），请统一在云防火墙的控制台中进行操作。

步骤3：编辑规则

在 企业安全组页面 下方，单击**入站规则**，可对已添加的规则进行编辑、插入、删除、快速排序等操作。

- **编辑规则：**在目标规则右侧，单击**编辑**，即可修改规则配置，修改完成后，单击**完成**即可。

- **停用规则：**在目标规则的状态栏，可以控制规则是否生效。若关闭开关，即停用规则，此规则不再参与规则匹配。

> **注意：**
> 企业安全组规则被停用后，安全组中的对应规则会被删除，但此规则依然会保留在企业安全组的规则列表中。

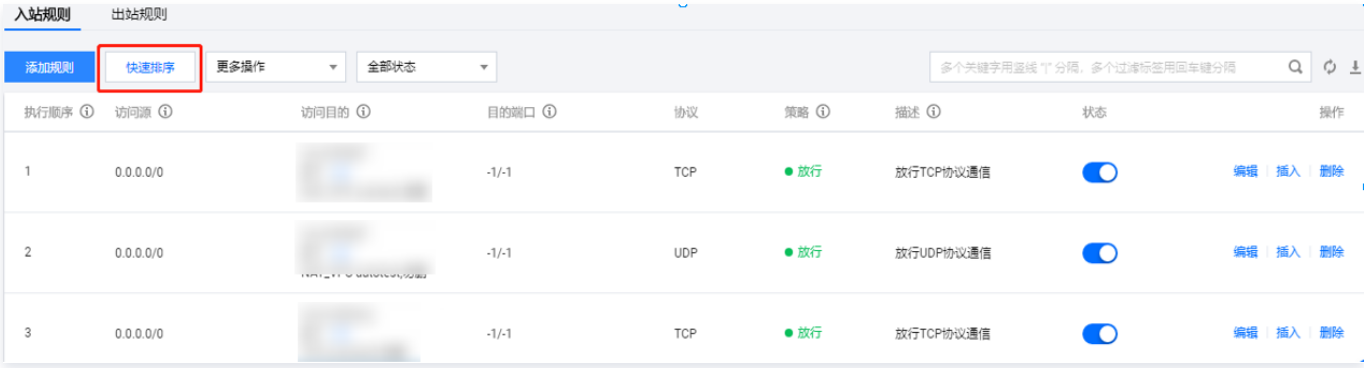
- **插入规则：**在目标规则右侧，单击**插入**，可在当前规则的前方新增一条规则，优先级高于当前规则。

- **删除规则：**在目标规则右侧，单击**删除**，二次确认后，可以删除目标规则。

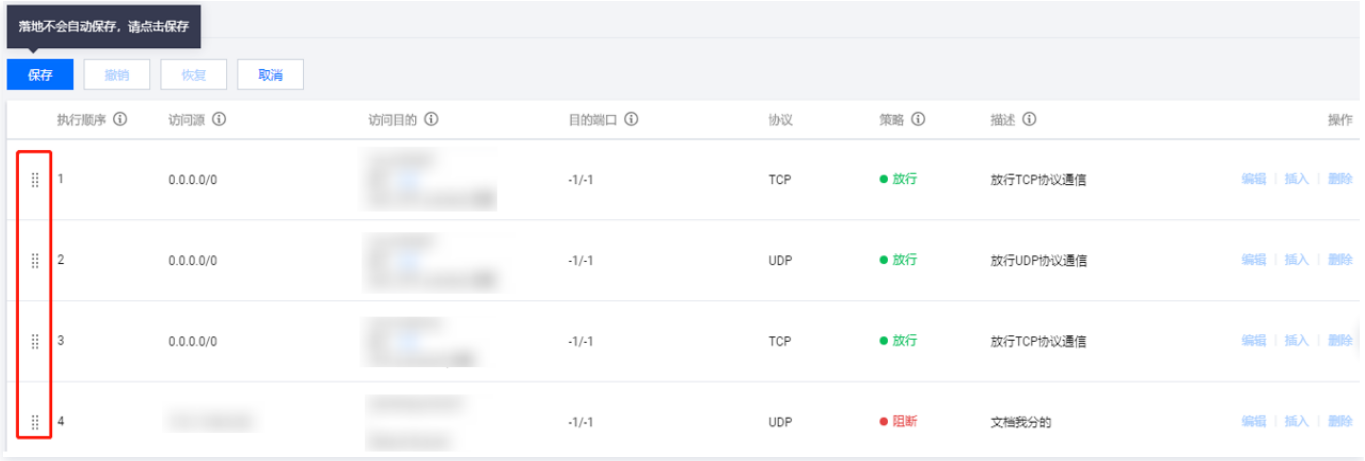
> **注意：**
> 删除规则后，企业安全组和安全组会同时删除此规则，且操作不可撤销。

- **快速排序：**

1.1 规则在列表中的顺序，决定了执行的优先级。在入站规则列表上方，单击**快速排序**。



1.2 可以通过对规则的拖拽操作，快速完成规则优先级的调整。



1.3 调整完成后，单击**保存**，调整后的优先级即可生效，企业安全组会自动将新的规则优先级下发到实例。

- **导出规则**：在规则列表的右上角，单击导出按钮，可以导出全量的入站规则或出站规则的 Excel文件。

> **注意：**
> 导出规则操作忽略了检索条件和规则开关状态。

常见问题

企业安全组到期后，云防火墙维护的安全组会被删除吗？

不会，云防火墙到期后，不会清除私有网络控制台中安全组配置。

可以在私有网络控制台，直接修改云防火墙维护的安全组吗？

不可以。在私有网络控制台手动修改后的安全组规则，不会体现在 企业安全组页面 中，容易产生规则管理上的纰漏，影响网络安全防护，同时企业安全组的规则更新后，会同步规则到安全组，手动修改的安全组配置会被覆盖。
更多企业安全组相关问题，可参见 安全可视 文档。

实例间单向访问的自动双向下发

最近更新时间：2024-11-04 22:00:22

自动双向下发功能用于实现内网到内网的通信，以两个内网主机的单向访问通信为例，介绍如何使用自动双向下发功能。

> **说明：**
> 云防火墙已推出新版企业安全组，新版企业安全组是在旧版的基础上做了一些改进，主要在配置项、逻辑等方面做了优化，规则匹配条件更加精细化，策略更加直观，便于理解和管理。推荐您可以使用 新版企业安全组，关于新旧版具体差异可以参见 热点问题。

前提条件

- 需已将云防火墙 升级到企业版或旗舰版。
- 首次使用企业安全组，需要已进行 CAM 授权。在您开通企业安全组后，首次进入**访问控制** > 企业安全组 **页面或访问控制日志** > 企业安全组 页面时，请按照提示进行授权操作。

  > **说明：**
  > 日志投递功能需要对云防火墙服务角色 CFW_QcsRole，关联策略 QcloudAccessForCFWRoleIn EnterpriseSecurityGroup 、QcloudAccessForCFWRoleInLogService 权限。

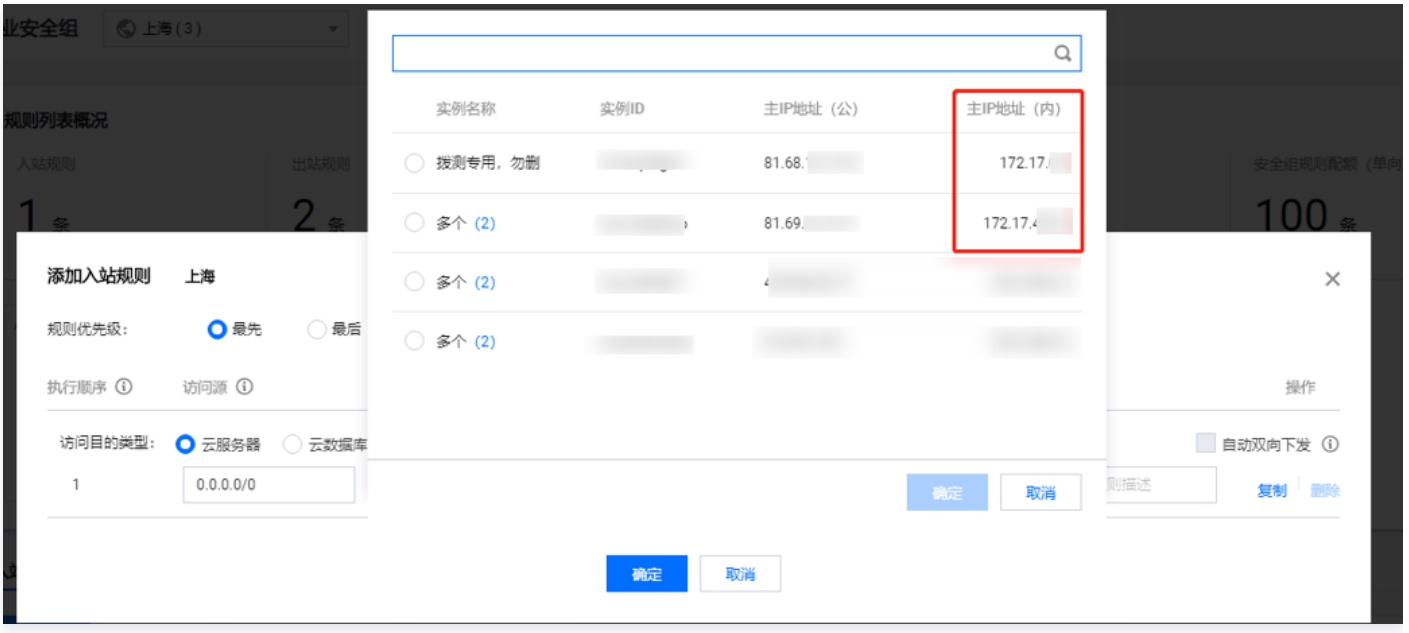
- 开通 CLS（日志服务）。当您完成 CAM 授权后，网络流日志会投递到您的腾讯云 CLS（日志服务）中。若您尚未开通此功能，请按照控制台提示，手动开启。开启 CLS 后，即可在刷新云防火墙的**访问控制日志** > 企业安全组 页面，查看相关日志内容。

操作步骤

1. 登录 云防火墙控制台，在左侧导航中，选择**访问控制** > **企业安全组**。
2. 在 企业安全组页面，左上角选择需要操作的地域。

   > **说明：**
   > 每个地域都有独立的企业安全组的入站规则列表和出站规则列表。

3. 在企业安全组页面下方，选择**入站规则** > **添加规则**。
4. 在添加入站规则的弹窗中，填写相关字段并选择两个内网主机。例如，只允许主机 A（内网 IP：172.17.xx.xx）访问主机 B（内网 IP：172.17.xx.xx）的规则。



5. 配置规则。第1条规则允许主机 A 访问主机 B，第2条规则禁止所有 IP 访问主机 B。由于第1条规则先执行，所以不会被第2条规则影响。

6. 勾选“自动双向下发”。
   - 由于第1条规则的访问源和访问目的都是内网 IP，所以此规则的“自动双向下发”功能是使能的，而第2条的访问源 IP 不是内网 IP，所以第2条规则，无法“自动双向下发”。
   - 实例对应多个 IP 时，勾选“自动双向下发”功能后，需要确认实例对应的 IP 数量，如果是 IP 对应多个实例，需要手动确定生效的实例。
7. 全部确认后，单击**确定**，即可在入站规则列表中，查看已添加的规则，同时出站规则列表中，由企业安全组自动生成了一条出站规则。

8. 添加完入站规则后，在私有网络控制台的 安全组页面 中，可查看企业安全组自动生成的安全组，自动配置了安全组规则和关联实例。

> **注意：**
> 请您不要手动修改云防火墙维护的安全组或路由表，统一在云防火墙的控制台中进行操作。

企业安全组(新)
配置步骤

最近更新时间：2025-05-15 16:09:12

概述

新版企业安全组在旧版的基础上做了比较大的调整，主要体现在以下几个方面：

- 去掉了地域限制和出入站方向的概念，只需定义好访问源和访问目的就可以实现安全组下发。
- 去掉了双向下发这个概念，默认自动双向下发规则，同时，如果不需要双向下发，可以通过在描述中添加关键字来实现单向下发的需求。
- 配置项新增了 IP/CIDR、地域等选项，各选项呈现对称排列，可以任意组合。
- 当访问源和访问目的类型设置为 IP 地址时，如果 IP 命中了实例就会进行自动同步。例如，在访问源或者访问目的输入全0的 IP 地址，就会同步所有的实例。
- 新版企业安全组配置比旧版更加简便，配置界面更加简洁，更加符合访问控制 ACL 的配置习惯。

> **注意：**
> 企业安全组与互联网边界防火墙是独立的。技术上，可以批量下发安全组设置到服务器或数据库上。即使未开启互联网边界防火墙或所购买的带宽不足，企业安全组仍可正常使用。

添加规则

1. 登录 云防火墙控制台，在左侧导航中，选择**访问控制** > **企业安全组(新)**。
2. 在企业安全组(新)页面，单击**添加规则**，弹出添加规则窗口。
3. 在添加规则窗口中，配置相关参数，单击**确定**。

参数说明

- 执行顺序：企业安全组规则的执行顺序，执行顺序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执行顺序时，原本该位置的规则的执行顺序+1，依次类推。当您删除某条规则时，后序所有规则的执行顺序-1。
- 访问源：IPv4规则支持 IP/CIDR、参数模板、资产实例、资产分组、资源标签、资产地域等类型。
- 访问目的：IPv4规则支持 IP/CIDR、参数模板、资产实例、资产分组、资源标签、资产地域、域名解析等类型。

> **说明**
> 当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。

- 目的端口：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”。
- 协议：当前版本支持UDP、TCP 和 ICMP 协议。

- 策略：
  - 放行：放通命中规则的流量，不记录企业安全组命中日志。
  - 阻断：拦截命中规则的流量，记录企业安全组命中日志。
- 描述：用于描述规则，最多支持50个字符，支持通过##的方式插入规则的特殊设置，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）。

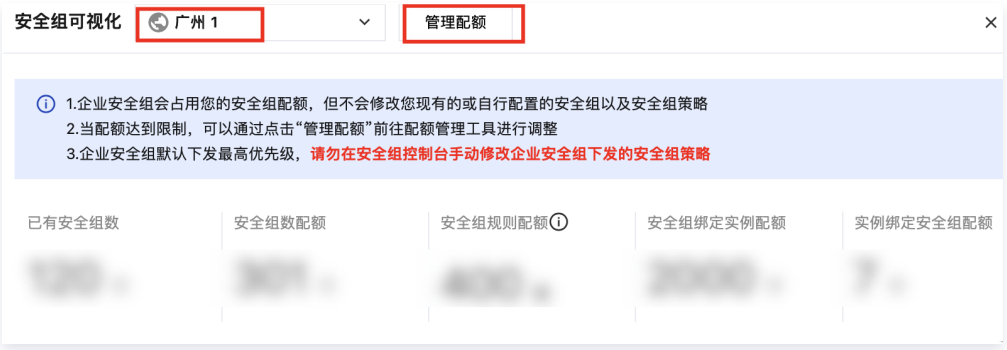
4. 规则添加完成后，将展示在规则列表里面。

5. 规则添加完并下发成功之后，在云防火墙的安全组可视化页面或者是进入私有网络控制台的 安全组页面 可以查看到相应的安全组，并且自动关联了实例。

查看安全组可视化

1. 登录 云防火墙控制台，在左侧导航中，选择**访问控制** > 企业安全组(新)。
2. 在企业安全组(新)页面，单击**安全组可视化**。

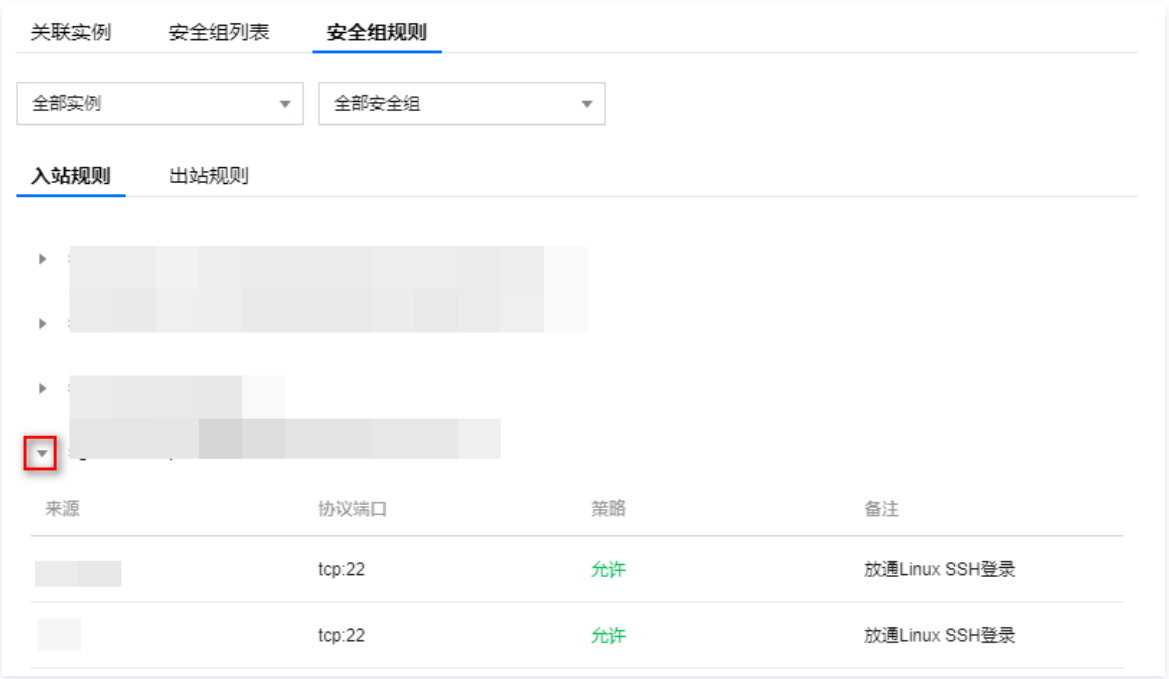
3. 在安全组可视化页面，可查看实例所在的地域和各种配额信息，安全组配额可以根据实际情况去扩容。



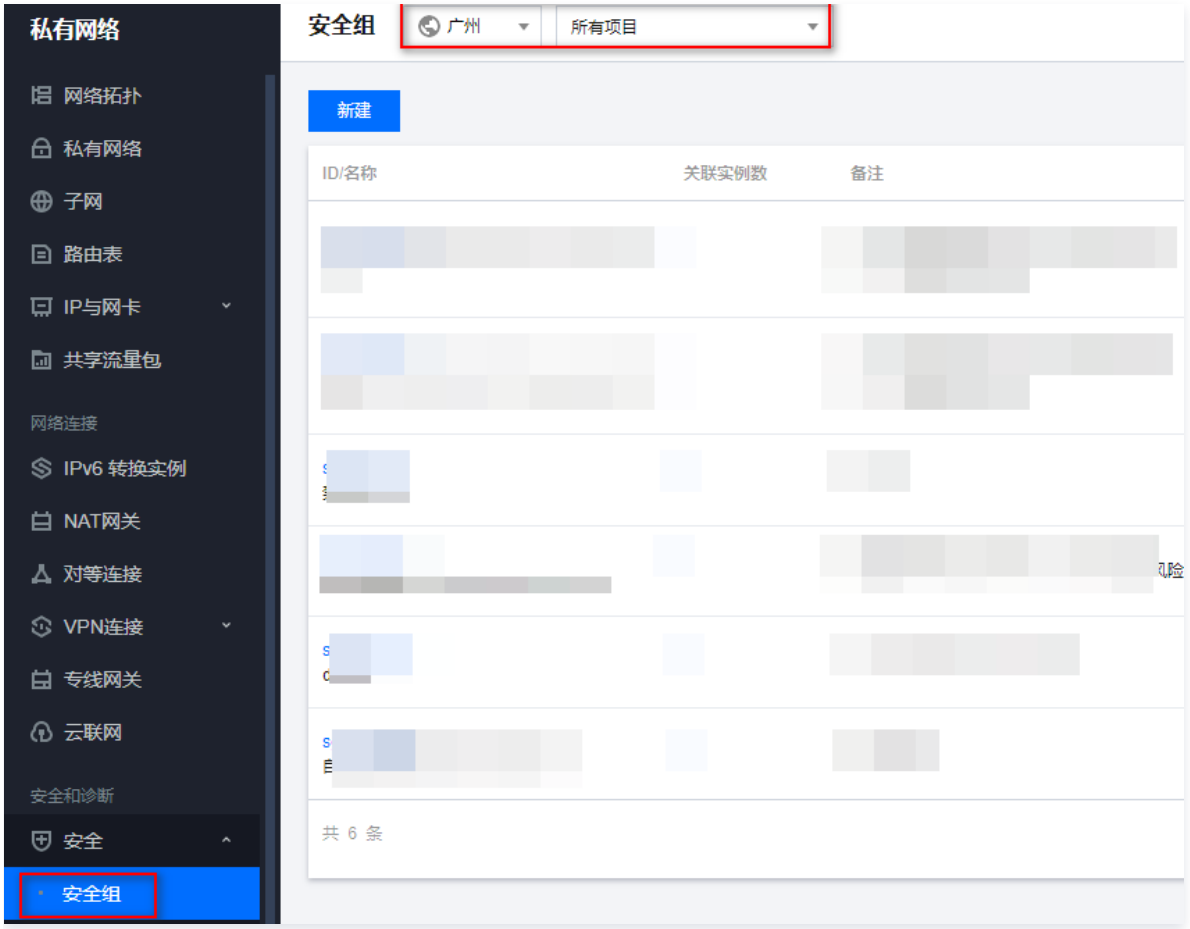
4. 在安全组可视化页面下方，可查看关联实例、安全组列表、安全组规则。
   - 关联实例：展示当前某个地域所有的实例，包括实例名称、实例类型、所属网络、IP 地址等信息。单击安全组或安全组规则列的“数字”，可以跳转到单个实例所对应的安全组列表或安全组规则详情页面。单击**查看详情**可以跳转到实例的详情页面。

- **安全组列表：展示了当前地域的所有安全组列表、每个安全组关联的实例、安全组规则条目数、创建时间等。单击关联实例或安全组规则列的“数字”，可以跳转到单个实例所对应的安全组列表或安全组规则详情页面。单击查看详情，可跳转到私有网络控制台安全组详情页面。**

- **安全组规则：展示当前地域所有安全组的入站规则和出站规则，单击 ▸ 可查看规则详情，也可验证企业安全组是否下发成功。**



5. 登录 私有网络控制台，在左侧导航中，选择**安全 > 安全组**，并选择所需地域和项目。



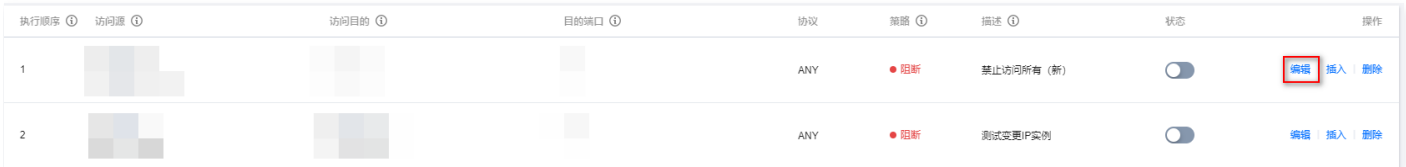
6. 单击任意一条安全组“ID/名称”，即可查看该安全组所对应的入站规则、出站规则以及关联的实例。

管理规则

企业安全组规则完成设置后，在企业安全组(新)页面可以对规则条目执行编辑、插入、删除操作、快速排序等操作。

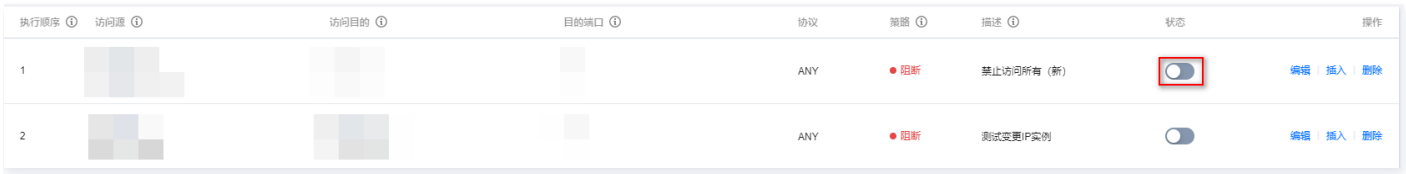
编辑规则

在 企业安全组(新)页面，选择所需规则，单击**编辑**，修改相关参数后，单击**确定**即可。



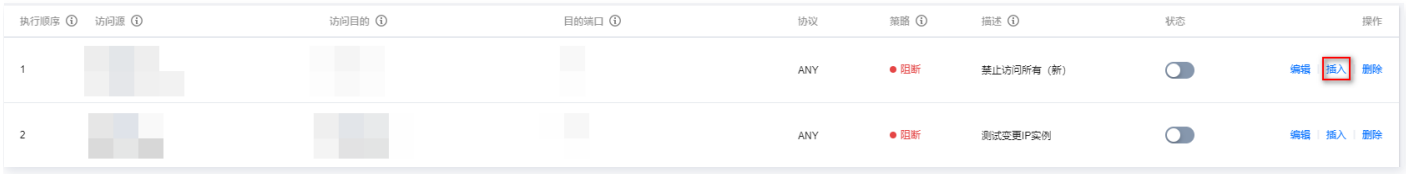
停用规则

在 企业安全组(新)页面，可以控制规则是否生效。若关闭开关，即停用规则，此规则不再参与规则匹配。



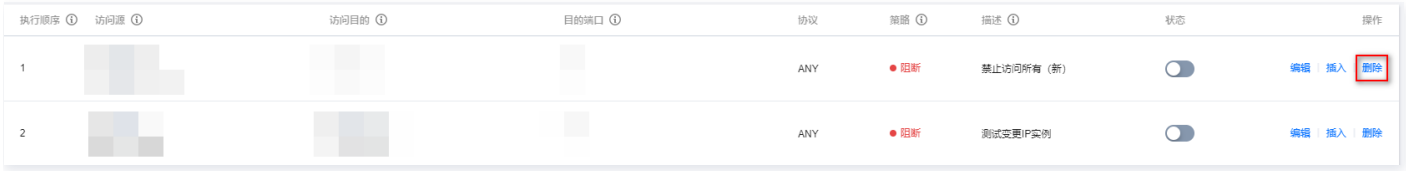
插入规则

在 企业安全组(新)页面，选择所需规则，单击**插入**，输入相关参数后，单击**完成**，可在当前规则的前方新增一条规则，优先级高于当前规则。



删除规则

在 企业安全组(新)页面，选择所需规则，单击**删除**，二次确认后，可以删除目标规则。



快速排序

规则在列表中的顺序，决定了执行的优先级。

1. 在 企业安全组(新)页面，单击**快速排序**，选择所需规则，点击鼠标左键拖拽至合适的位置。

2. 调整完成后，单击**保存**，调整后的优先级即可生效，企业安全组会自动将新的规则优先级下发到实例。

导出规则

1. 在 企业安全组(新)页面，单击规则列表右上方的 ，弹出自定义列表导出窗口。

2. 在自定义列表导出窗口中，选择忽略检索条件全量导出或基于检索条件导出，单击**导出**，即可导出规则。

自定义列表导出
忽略检索条件全量导出
基于检索条件导出
执行顺序
规则ID
访问源
访问目的
目的端口
协议
策略
描述
状态
导出
取消

企业安全组流日志

最近更新时间：2024-11-15 09:14:41

功能简介

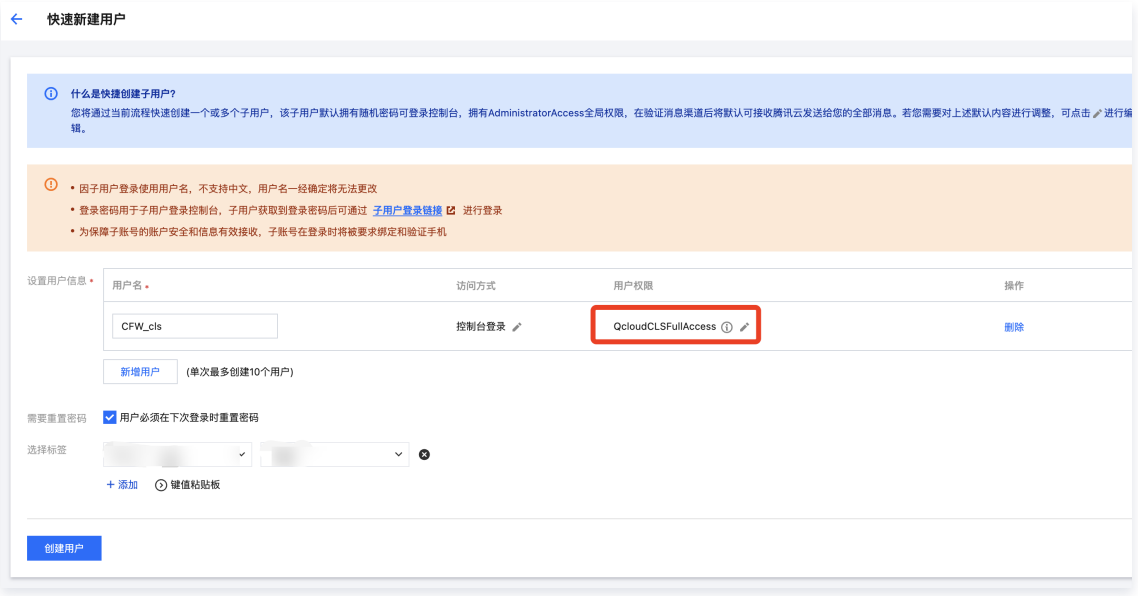
企业安全组流日志将实时记录所有经过的安全组规则的流量情况，包括拦截和观察规则，可以配合企业安全组完成云上隔离和内网流量审计。

> **说明：**
> 旗舰版以下用户请 提交工单 申请使用企业安全组流日志。

配置指引

企业安全组日志依赖网络流日志，需要从您的 CLS 中采集原始日志信息进行加工处理，所以需要您创建有 CLS 权限的角色并授权 CLS 采集网络流日志。

1. 使用**主账号**进入 访问管理-用户列表页面，为防火墙日志投递任务创建专属 API 调用账号，创建新用户并赋予 CLS 的全读写权限（QcloudCLSFullAccess）更多详情请参见 创建子用户-快速创建 。

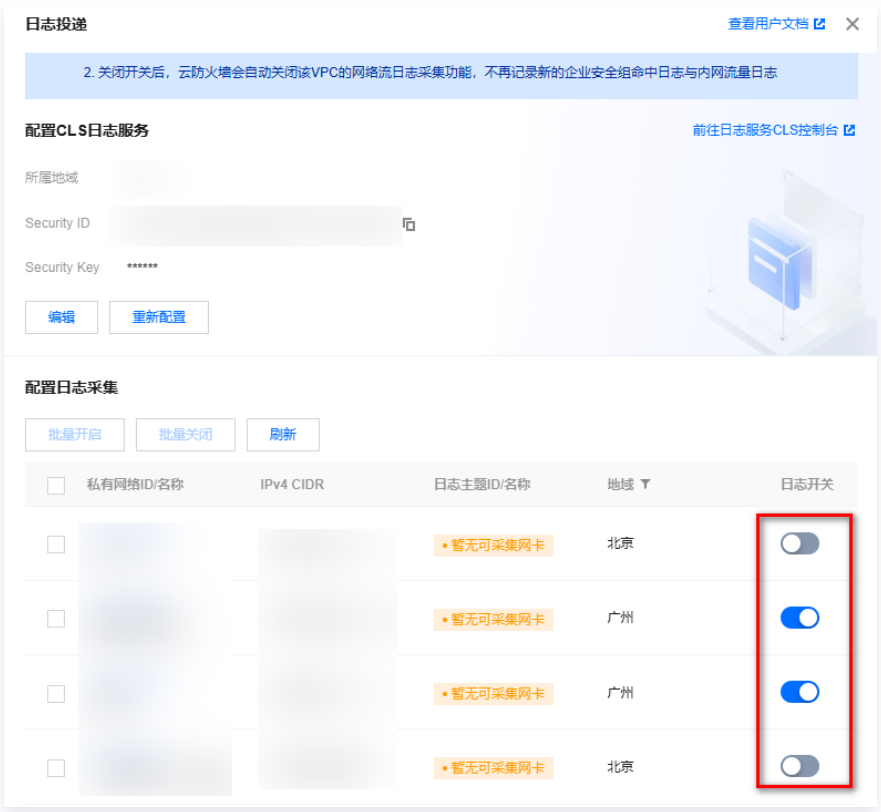


2. 在 访问控制-企业安全组页面，单击**企业安全组日志**的**设置详情**。
3. 在采集企业安全组日志页面，单击**配置 CLS 日志服务**的**编辑**，填写 SecurityID 和 SecurityKey 进行身份认证，单击**保存**。

4. 参考 文档，前往 角色页面 授权采集网络流日志 ，授权流日志访问 CLS 权限 QcloudAccessForVPCRoleInFlowLogAdvanceAnalysis。

5. 在 访问控制-企业安全组页面，单击企业安全组的**流日志开关**，启用流日志功能。

6. 单击**设置详情**，开启需要采集内网间流量的 VPC 开关。



实践教程

场景一：审计安全组拦截命中

> **说明：**
> 排查命中阻断策略的安全组，定位具体是哪一条安全组规则阻断流量。

1. 出现流量被安全组拦截，需要定位具体拦截的规则时。
2. 在 访问控制-企业安全组页面，单击企业安全组的**日志设置**，打开需要排查的 VPC 对应开关，企业安全组会自动记录安全组的阻断命中日志。
3. 复现被拦截的流量连接请求，在 访 问控制日志-企业安全组 流日志中，根据访问源/访问目的进行筛选，定位命中阻断策略的安全组规则。

场景二：VPC 内（子网间、子网内）流量监控

> **说明：**
> 监控所有 VPC 内的流量，包括子网间、子网内的流量。

1. 在 访问控制-企业安全组页面，单击企业安全组的**日志设置**，打开需要排查的 VPC 对应开关。
2. 企业安全组流日志会自动记录该 VPC 内所有流量情况，包括子网间访问流量和子网内流量。

3. 在 流量日志-内网流量日志页面，对子网间、子网内的流量进行记录排查。

场景三：VPC 间流量监控

> **说明：**
> 监控所有进出 VPC 的内网流量。

1. 在 访问控制-企业安全组页面，单击企业安全组的**日志设置**，打开需要排查的 VPC 对应开关。
2. 企业安全组流日志会自动记录进出该 VPC 内所有流量情况。
3. 在 流量日志-内网流量日志页面，对该 VPC 的进出流量进行记录排查。

迁移指南

最近更新时间：2024-05-17 15:49:31

若已使用旧版企业安全组，可以通过如下操作将旧版企业安全组的规则迁移至新版中。

迁移思路

1. 设置规则开关不自动开启。
2. 梳理旧版企业安全组策略。
3. 配置迁移到新版企业安全组。
4. 开启新版企业安全组开关。
5. 验证策略是否下发成功并生效。
6. 验证没问题后，删除旧版企业安全组规则。
7. 完成迁移。

> **注意：**
> 迁移有风险，请一定仔细确认 验证策略 是否下发成功并生效。

步骤1：设置规则开关不自动开启

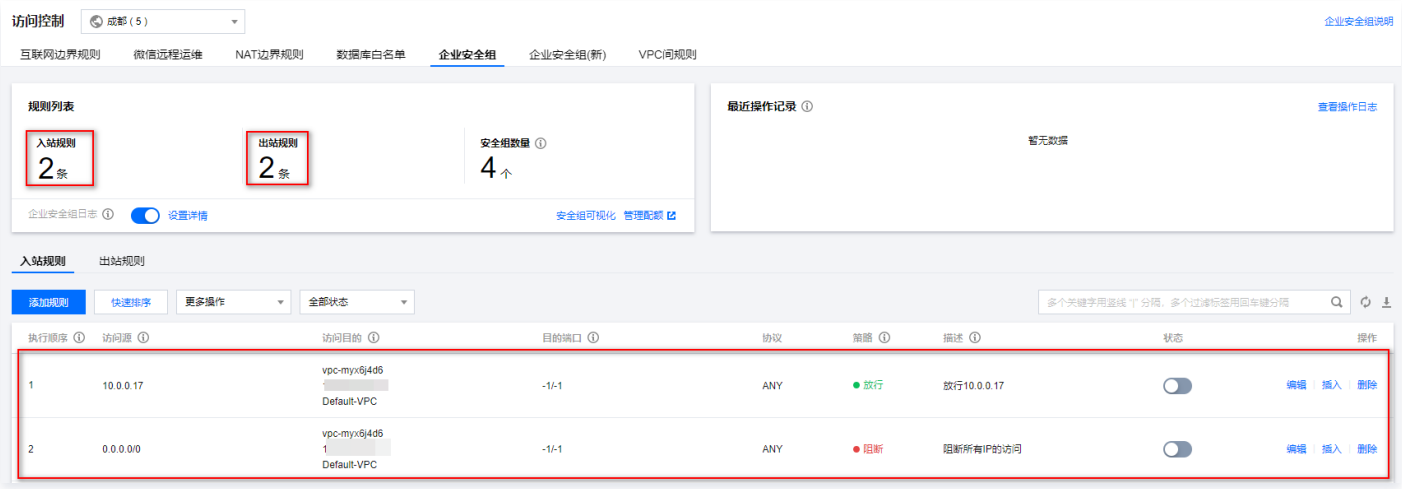
建立新版企业安全组规则之后，规则开关不会自动开启，需要手动去开启，从而做到控制安全组策略的下发，避免规则配置错误影响业务，具体配置如下：

1. 登录 云防火墙控制台，在左侧导航单击**通用设置**，进入通用设置页面。
2. 在通用设置页面，下翻找到访问控制规则设置项，选择**默认不启用**。

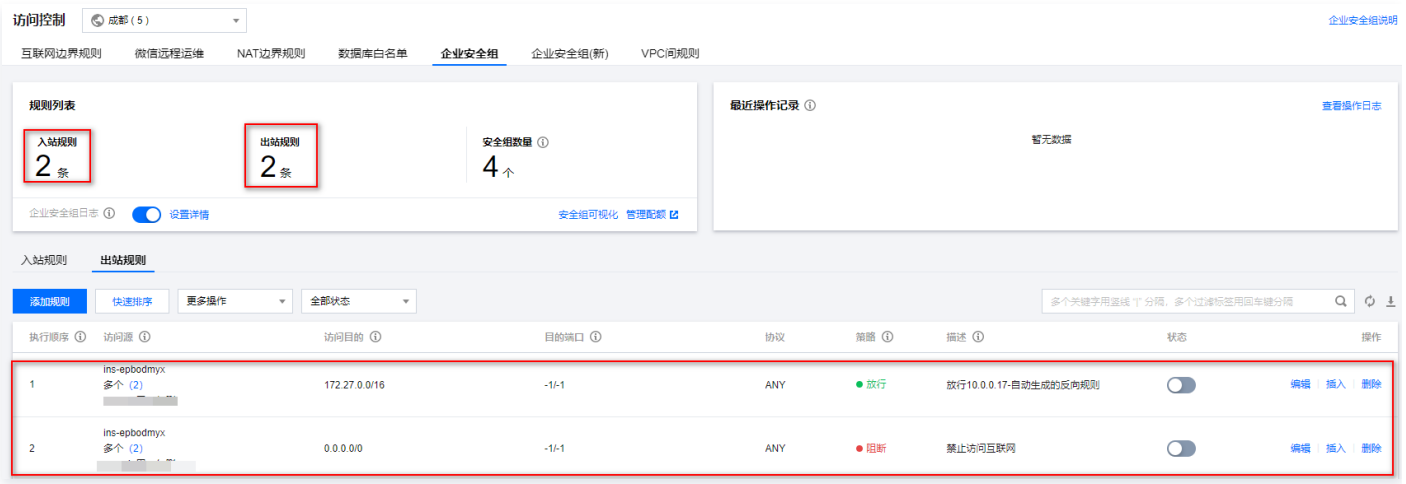
步骤2：梳理旧版企业安全组策略

明确旧版企业安全组的出入站规则，有哪些规则是双向的、单向的、怎样配置的，为制定新版企业安全组规则做准备。将通过一个举例来演示一下规则迁移的步骤。具体详情如下：

1. 在 企业安全组 > **入站规则**页面，显示成都地域配置了2条入站规则和2条出站规则。其中，入站规则第一条针对 `vpc-myx6j4d6` 这个实例设置了一条入站策略，允许 `10.0.0.17` 访问，第二条也设置了一条入站策略，禁止所有其他 IP 访问。



2. 单击**出站规则**切换页面，很明显第一条规则是入站创建规则时勾选了双向下发自动生成的，即针对 `ins-epbodmyx` 这个访问源自动生成了一条允许访问 `vpc-myx6j4d6` 这个实例的出站规则，第二条规则是手动设置一条禁止 `ins-epbodmyx` 访问其他 IP 的规则。



3. 以上就是对旧版企业安全组规则分析的一个举例，具体每个环境中要根据实际情况去分析。分析完成之后，需要把规则迁移到新版企业安全组了。

步骤3：迁移到新版企业安全组

根据上面的例子，将介绍新版企业安全组该如何去配置才能实现相同的效果。

1. 首先，为您介绍新版企业安全组配置界面做了哪些改动，如下图所示，新版增加了 IP、地域等配置项目，可以实现两个 IP 段之间访问控制以及 IP、资产实例、资产分组到地域等双向的访问控制。

2. 介绍了新版的配置规则之后，再来看到上述两个出入站场景规则该如何配置。入站策略配置要点有两条：一条允许 `10.0.0.17` 访问 `vpc-myx6j4d6`；一条禁止所有 IP 访问 `vpc-myx6j4d6`，具体配置如下图所示：

2.1 在 企业安全组(新)页面，单击**添加规则**，弹出添加规则窗口。

2.2 在添加规则窗口中，配置相关参数，单击**确定**。

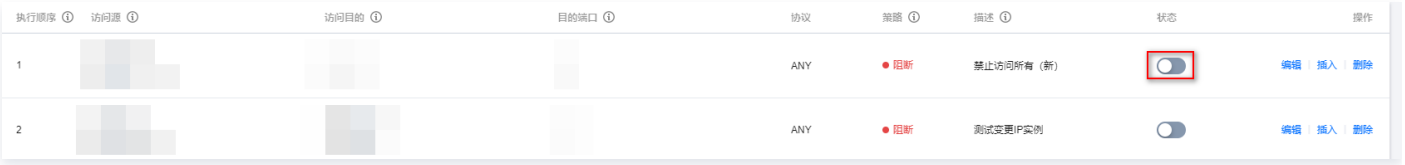
参数名称	第一条规则	第二条规则
访问源类型	IP/CIDR	IP/CIDR
访问目的类型	选择资产实例	选择资产实例
端口协议类型	自定义	自定义
规则优先级	自定义	自定义
访问源	10.0.0.17	0.0.0.0/0
访问目的	vpc-myx6j4d6	vpc-myx6j4d6
目的端口	所有	所有
协议	所有	所有
策略	放行	阻断
描述	自定义	自定义

3. 等待几秒钟下发到资产的安全组，即可将旧版企业安全组策略迁移至新版企业安全组。

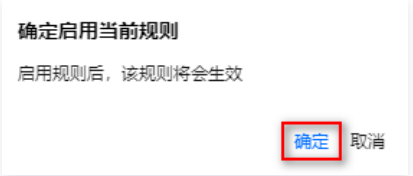
步骤4：开启新版企业安全组开关

开启新版安全组规则的开关，使该规则生效。

1. 在 企业安全组(新)页面，选择所需规则，单击状态列下的 ，弹出“确认开启”弹窗中，单击**确定**，该规则即可生效。



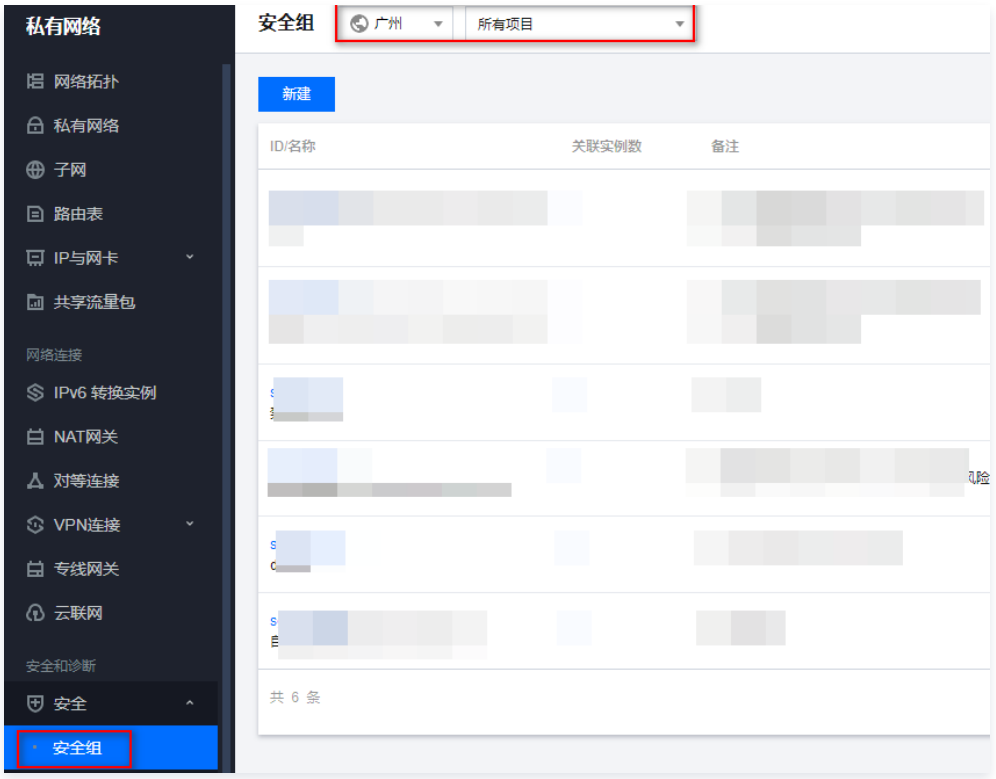
2. 在“确认开启”弹窗中，单击**确定**，该规则即可生效。



步骤5：验证策略是否下发成功并生效

启用规则后，需要去实例的安全组看一下策略是否下发成功。

1. 登录 私有网络控制台，在左侧导航中，选择**安全 > 安全组**，并选择所需地域和项目。



2. 在安全组页面，红框标出来的安全组策略是通过企业安全组下发的，底下标注了 cfwsg 字样也代表该规则是通过云防火墙创建的。

3. 单击任意一条安全组“ID/名称”，验证一下上述规则是否下发成功，如下图所示，两条入站规则下发成功。

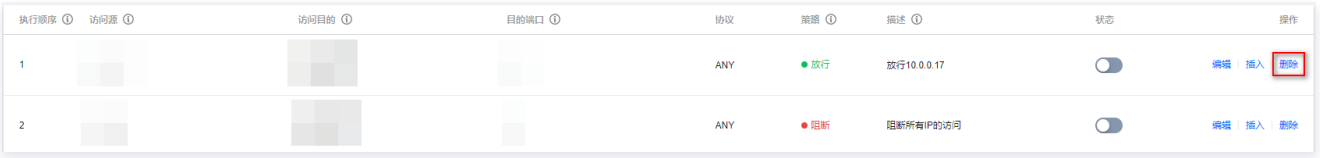
4. 单击**出站规则**切换页面，如下图所示，出站规则也是下发成功了。

> **说明：**
> 第一条规则是自动双向下发生成的，即在 `vpc-myx6j4d6（172.27.0.0/16）` 的入站方向创建了一条允许 `10.0.0.17` 访问的规则，相应的针对 `10.0.0.17`，会在它的出站方向自动生成一条允许访问 `vpc-myx6j4d6（172.27.0.0/16）` 的出站规则。第三条禁止访问所有的规则也已经下发成功。

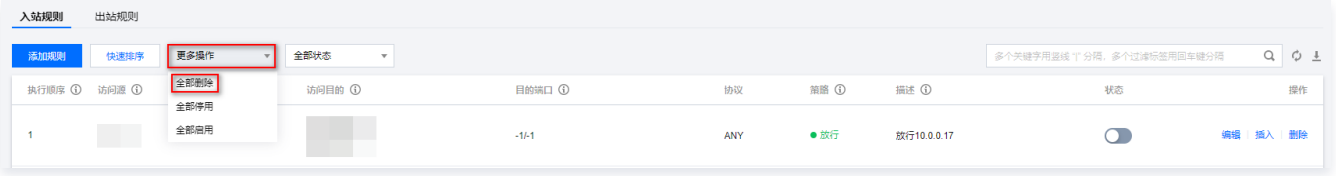
步骤6：删除旧版企业安全组规则

通过上述验证新版规则下发没问题之后，就可以把旧版的规则删除。

1. 在 企业安全组 > **入站规则**页面，支持删除单个或全部规则，具体操作如下所示。
   - 单个：选择所需规则，单击操作列的**删除**，弹出“确认删除” 窗口。



   - 全部：单击**更多操作 > 全部删除**，弹出“确认删除” 窗口。



2. 在“确认删除” 窗口中，单击**确定**，即可删除规则。

步骤7：完成迁移

以上就是关于企业安全组从旧版迁移新版的方法介绍，后续可在 企业安全组(新)页面 新增安全组规则，详情操作请参见 配置步骤 。

热点问题

最近更新时间：2023-09-22 14:13:02

为什么要推出新版企业安全组?

老版本企业安全组在配置和管理方面比较繁琐，新版企业安全组是在旧版的基础上做了一些改进，主要在配置项、逻辑等方面做了优化，规则匹配条件更加精细化，策略更加直观，便于理解和管理。

新版企业安全组相较于旧版企业安全组有哪些优势?

新版本企业安全组具有如下特点：

- 取消了双向下发按钮，配置规则时会自动生成一条入站规则和一条出站规则。
- 取消了入站规则和出站规则方向概念，只需要定义好访问源和访问目的即可完成规则的配置。
- 取消了地域的限制，所有规则展示在同一个界面，更加便于运维管理。
- 配置项新增了 IP/CIDR、地域等选项，各选项呈现对称的排列，可以任意组合。
- 新增访问源或者访问目的配置的是 IP 地址时，会自动命中 IP 所对应的实例。

两个版本企业安全组是否可以共存?

新老版本的企业安全组功能可以共同使用，但是新版本企业安全组优先级要高于老版本，如果配置了新版企业安全组策略，策略匹配顺序将先匹配新版再匹配旧版。

旧版企业组是否可以继续使用?

推出新版企业安全组功能后，旧版会继续提供服务，可以继续使用。

旧版企业组规则怎么迁移到新版企业安全组?

关于将旧版企业组规则迁移到新版企业安全组的详细操作，详情请参见 迁移指南 。

特殊应用场景

最近更新时间：2024-05-17 15:49:31

本文将为您介绍云防火墙的访问控制功能的特殊应用场景。

管理规则列表的执行顺序

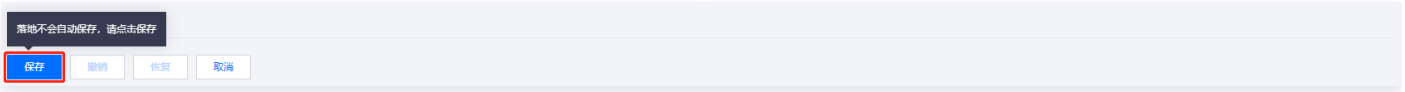
互联网边界规则、NAT 边界规则及 VPC 间规则都支持管理规则列表的执行顺序，接下来将以“互联网边界规则”为例进行说明。

场景1：对列表内规则进行快速排序

1. 登录 云防火墙控制台，在左侧导航栏中，选择**访问控制** > **互联网边界规则**。
2. 在互联网边界规则页面的规则列表上方，单击**快速排序**，列表进入编辑模式。

3. 用户能够在当前页面范围内，批量移动规则的位置和顺序，通过拖动规则前方图标，对规则进行排序。

4. 移动完成后需单击**保存**即可生效。



排序操作说明：

- 每次松开鼠标后，导致**位置**发生变化的规则落地，视为一次排序操作。
- 松开鼠标后，**位置**没有发生变化，则不是一次排序操作。
- 发生过一次排序操作后，**撤销**按钮亮起。
- 单击一次**恢复**，列表回到上一次排序操作后的状态。
- 单击**保存**，完成后，页面上方会出现排序**完成**提示。
- 单击**取消**，列表会回到初始状态，所有排序操作不生效。

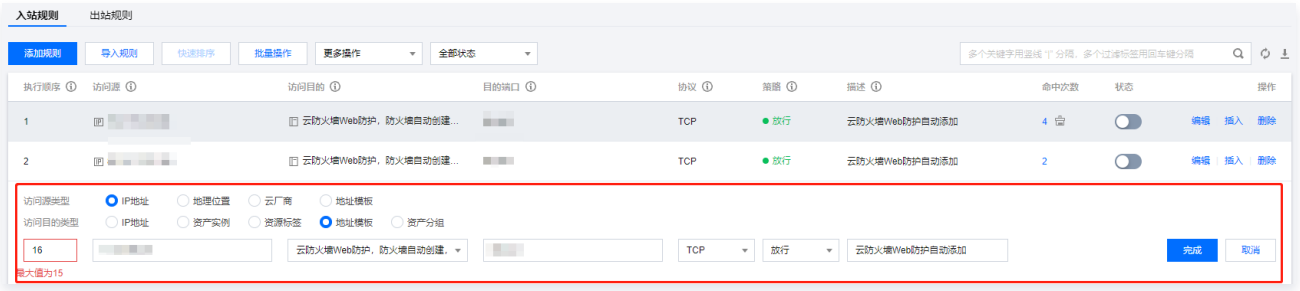
场景2：通过编辑将规则移动至指定位置

当需要大范围的移动某条规则时，快速排序功能不能高效的执行这一类操作，因此，通过编辑可以快速的将当前规则移动到指定的位置，与快速排序不同，编辑功能一次只能实现对一个规则执行顺序的修改。

1. 登录 云防火墙控制台，在左侧导航栏中，选择**访问控制** > **互联网边界规则**，进入互联网边界规则页面。
2. 在互联网边界规则页面的规则列表中，找到需要移动的规则，确定移动的期望位置。

3. 在规则右侧，单击**编辑**，进入规则编辑模式。
4. 修改执行顺序字段的值，修改为期望位置的执行顺序值。

> **注意：**
> 由于执行顺序的不可重复原则与连续原则，通过编辑进行规则的移动时，执行顺序的合理输入最小值为1，最大值为当前列表中的规则数量。



5. 单击**完成**，检查列表中的规则顺序是否符合预期。

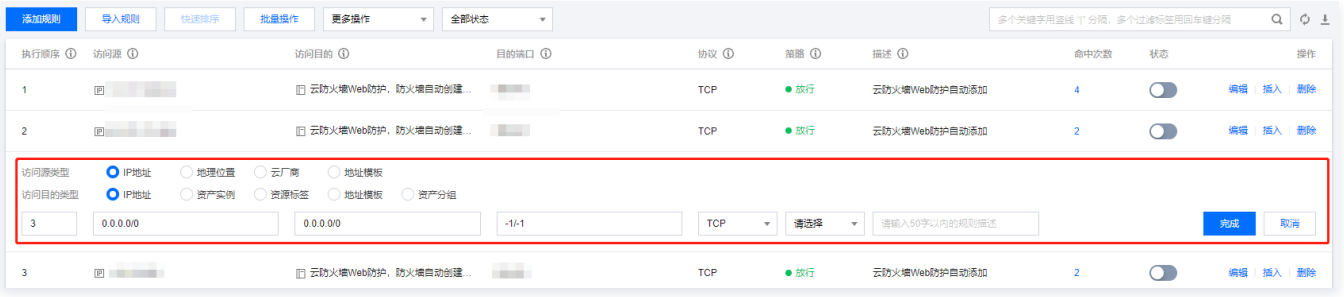
> **说明：**
> 通过编辑规则可以实现移动规则在列表中的位置，从而直接将该规则的执行顺序调整到期望的位置，其他所有规则也会自动移动调整。

场景3：在现有列表中的指定位置插入一条规则

云防火墙支持在任意两条规则之间，插入一条规则，插入规则的执行顺序即为当前插入的位置。
规则采用**前插**的方式，若需要在执行顺序为“2”和“3”的规则之间，插入一条新的规则：

1. 登录 云防火墙控制台，在左侧导航栏中，选择**访问控制** > **互联网边界规则**，进入互联网边界规则页面。
2. 在互联网边界规则页面的规则列表中，找到执行顺序为“3”的规则，在规则右侧单击**插入**。
3. 将在执行顺序为“3”的规则上方，弹出规则编辑框。
4. 在规则编辑框中，填写规则字段，单击**完成**即可完成规则插入。

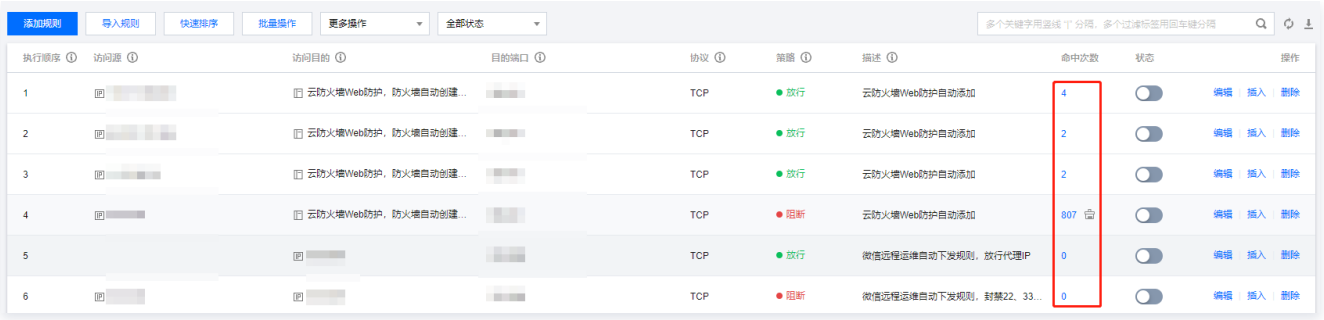
> **说明：**
> 完成插入操作后，被插入规则的执行顺序取代下方那条规则的执行顺序，而插入规则下方所有规则的执行顺序均“+1”。



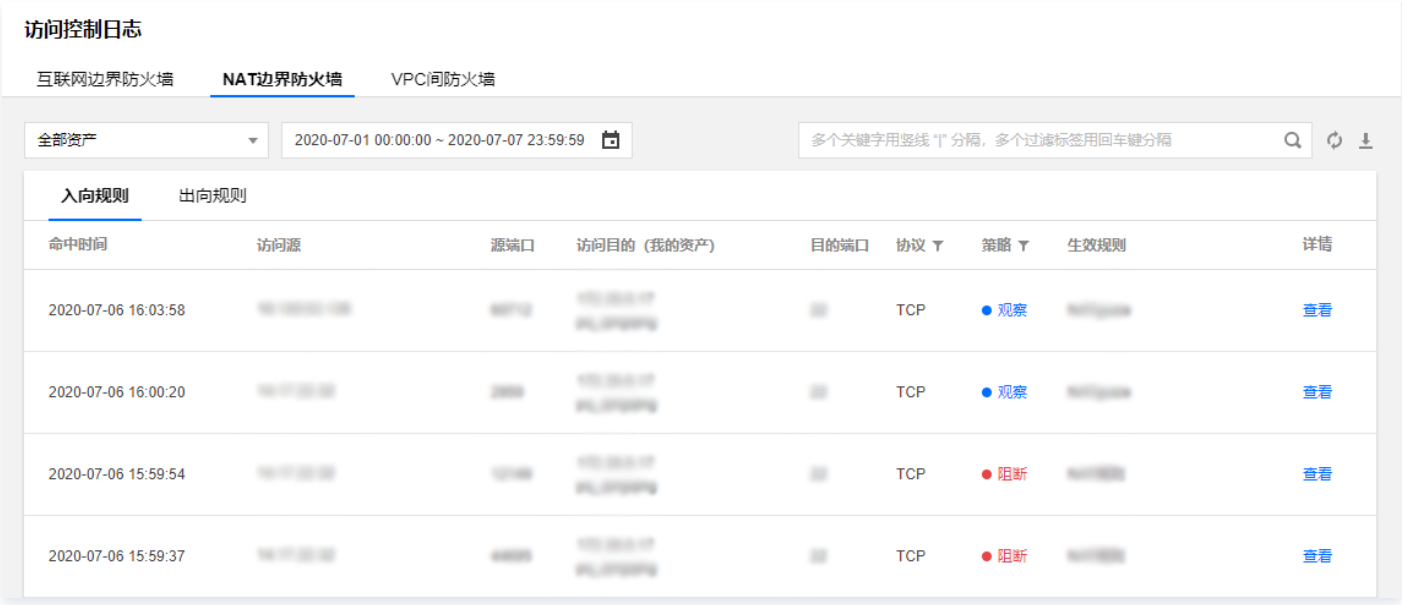
查看规则是否生效

- **方式1**：查看访问控制列表中的命中次数，若有命中次数，则表示规则生效。

> **说明：**
> 若规则命中次数为零，只能说明暂时没有被命中，可以理解为暂时没有生效，但是不代表规则配置有误。



- **方式2：左侧导航栏中，选择日志审计 > 访问控制日志，查看访问控制日志（规则命中记录日志），若在访问控制日志中，查看到相关规则，则表示该规则生效。**



操作锁

同一个 AppID 的同一张访问控制列表（VPC 使用防火墙 ID 来区分），在同一时间只允许一个用户执行**添加规则**、**导入规则**、**快速排序**、**编辑**、**插入**中的任意一个操作。
当用户对列表进行操作时，如在页面上方出现：“列表可能正在被其他人操作，已被锁定，请稍后重试”的提示时，则代表此时有其他的用户正在对该列表进行操作。

> **说明：**
> 操作锁的有效期为5分钟，到时后自动释放。

相关信息

如遇到访问控制相关问题，可参见 访问控制 文档。

访问控制概述

最近更新时间：2025-05-16 10:19:22

访问控制资产

云防火墙可保护的资产范围覆盖云环境中的多种资源类型：

资产类型	说明
公网 IP	包括 CVM 实例绑定的公网 IP、弹性公网 IP（EIP）、负载均衡（CLB）的公网出口等
内网 IP	包括 CVM 实例、TKE 节点绑定的内网IP等
服务器实例	包括 CVM 实例、LH 实例等
域名	包括公网域名、内网域名等

访问控制方式

云防火墙支持按照以下方式配置访问控制规则：

访问控制方式	说明
IP 规则	基于IPV4、IPV6进行访问控制，支持精确匹配或 CIDR 网段配置
域名规则	基于 FQDN 功的灵活域名流量管控，根据访问中请求的域名，判断是否放行，不校验域名解析的 IP
域名解析规则	根据协议、实例所在的地域，放行域名实际请求的 IP
资源标签规则	基于腾讯云资源标签批量管理访问权限
地址模板规则	使用预定义的 IP 地址模板快速配置规则
地理位置规则	根据 IP 地址的地理归属（国家、地区）限制访问
云厂商规则	针对特定云服务商的 IP 范围或服务标签进行控制

版权所有：腾讯云计算（北京）有限责任公司

入侵防御
开启威胁情报

最近更新时间：2023-09-22 14:13:03

开启威胁情报后，云防火墙会将互联网边界流量接入威胁情报检测与分析引擎，识别访问控制规则以外的未知风险。针对重保场景，推出了重保情报包功能，加强了风险抵御能力。

操作步骤

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，单击威胁情报处的，将开启威胁情报。

> **注意**
> 威胁情报开关与 互联网边界防火墙 开关是复合逻辑开关，只有当某个公网 IP 开启了互联网边界防火墙开关，并开启威胁情报开关后，云防火墙才会对该公网 IP 的南北向流量进行威胁情报的监控与分析。

3. 开启威胁情报后，云防火墙会将互联网边界流量接入威胁情报检测与分析引擎，识别访问控制规则以外的未知风险：
   - 外部恶意访问：监控并识别来自外部的恶意扫描、暴力破解、挖矿木马、勒索软件、远程控制等恶意 IP 和威胁样本，对云上资产发起的访问。
   - 主动外联行为：监控并识别云上资产向外部恶意 IP 地址或域名发起的主动外联，并根据威胁情报提供的大数据对比分析，判断可能发生的主机失陷风险。
4. 开启重保专题情报包功能，重保专题情报包是针对重保期间通过攻防队众包的方式形成的，在 入侵防御页面，单击威胁情报处的**查看详情**，单击开启重保专题情报包开关，开启后匹配情报包中的 IP 都会自动加入封禁列表，拦截所有的访问行为。

> **说明**
> 重保专题情报包功能仅支持购买 云防火墙旗舰版 用户使用。

相关信息

如遇到入侵防御相关问题，可参见 入侵防御 文档。

开启基础防御

最近更新时间：2024-04-22 17:25:32

版权所有：腾讯云计算（北京）有限责任公司

开启基础防御后，可对公网 IP 的南北向流量进行入侵防御规则的检测。

操作步骤

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到“基础防御”模块，单击**查看规则**，将弹出基础防御规则列表弹窗。

3. 在基础防御规则列表弹窗内，可以查看腾讯云 IPS 规则列表，单击**规则 ID**，即可查看相应规则描述。

4. 单击开关处，可以指定规则对于 NAT 和 VPC 防火墙是否生效。

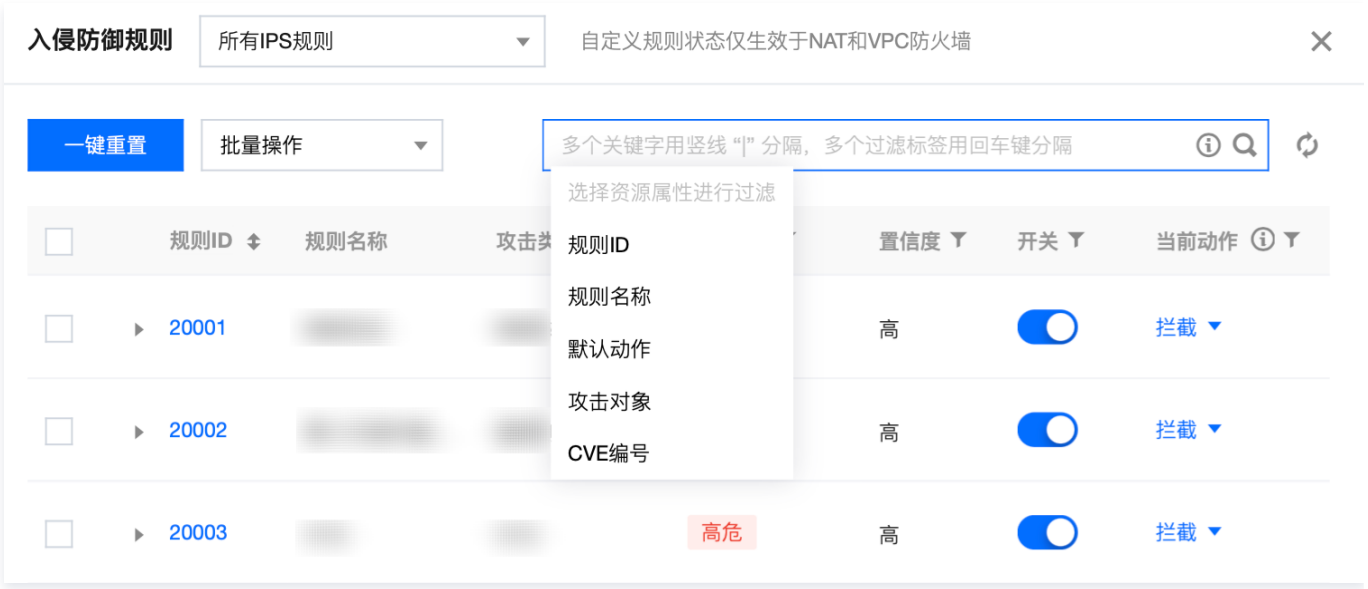
> **注意：**
> 如果您的部分防火墙引擎版本过低，则对应防火墙将不会生效。

5. 在当前动作列中，可以选择命中规则后的规则动作，规则动作仅生效于防护模式为拦截模式的资产。

注意：

自定义入侵防御规则功能仅针对企业版及以上客户生效，且仅生效于 NAT 边界防火墙和 VPC 边界防火墙。如果您的部分防火墙引擎版本过低，则对应防火墙将不会生效。

6. **对于所有 IPS 规则，支持按关键字查询、一键重置、批量操作。**
   - **按关键字查询：支持按照规则属性对相应规则进行查询，从而进行开关状态设置与处置动作设置。**



- 一键重置：支持一键恢复所有规则的开关状态并切换动作为默认动作，即时生效。

- 批量操作：支持选中多个规则，批量启用、停用，或是切换处置动作。

7. 了解规则后，在“基础防御”模块，单击基础防御处的，将开启基础防御。

> **说明：**
> - 关闭“基础防御”开关后，所有基础防御规则将不再生效。
> - 基础防御开关与 互联网边界防火墙 开关是复合逻辑开关，只有当某个公网 IP 开启了互联网边界防火墙开关及基础防御开关后，云防火墙才会对该公网 IP 的南北向流量进行入侵防御规则的检测。
> - 在拦截模式下，针对部分高置信度的规则支持自动拦截，其他规则仍然产生安全事件告警。

相关信息

如遇到入侵防御相关问题，可参见 入侵防御 文档。

开启虚拟补丁

最近更新时间：2024-04-22 17:25:32

开启虚拟补丁后，云防火墙会对南北向流量中，所有可被漏洞利用和攻击的流量，进行自动识别和拦截，从而避免云服务器中的漏洞暴露在互联网。

操作步骤

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到“虚拟补丁”模块，单击**查看规则**，将弹出虚拟补丁规则列表弹窗。

3. 在虚拟补丁规则列表弹窗内，可以看到所有被应用的补丁规则，单击**规则 ID**，即可查看该补丁规则的应用描述。

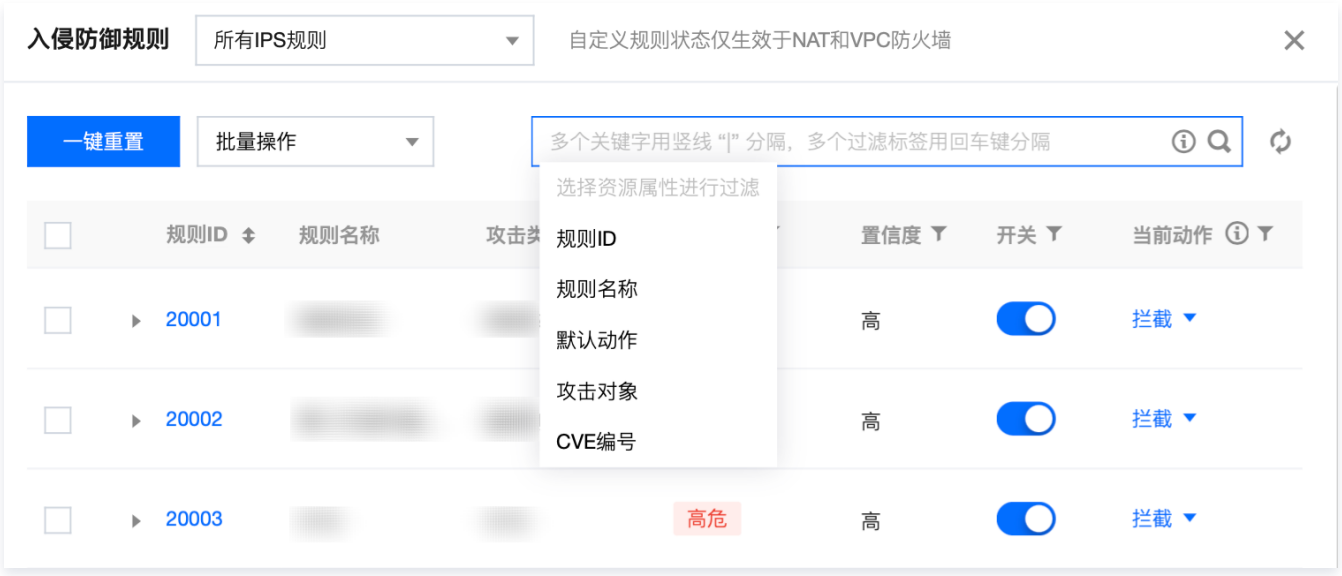
4. 单击开关处，可以指定规则对于 NAT 和 VPC 防火墙是否生效。

> **注意：**
> 如果您的部分防火墙引擎版本过低，则对应防火墙将不会生效。

5. 在当前动作列中，可以选择命中补丁规则后的规则动作，规则动作仅生效于防护模式为拦截模式的资产。

> **注意：**
> 自定义入侵防御规则功能**仅针对企业版及以上客户生效**，且仅生效于 NAT 边界防火墙和 VPC 边界防火墙。如果您的部分防火墙引擎版本过低，则对应防火墙将不会生效。

6. **对于所有 IPS 规则，支持按关键字查询、一键重置、批量操作。**
   - **按关键字查询：支持按照规则属性对相应规则进行查询，从而进行开关状态设置与处置动作设置。**



- 一键重置：支持一键恢复所有规则的开关状态并切换动作为默认动作，即时生效。

- 批量操作：支持选中多个规则，批量启用、停用，或是切换处置动作。

7. 查看完补丁规则后，在“虚拟补丁”模块，单击虚拟补丁处的，将开启虚拟补丁。

> **注意：**
> - 虚拟补丁开关“开启”状态下，虚拟补丁的对应规则对开启开关的公网 IP 生效。
> - 虚拟补丁开关“关闭”状态下，虚拟补丁的对应规则不生效。
> - 在拦截模式下，自动阻断所有入侵活动。

相关信息

如遇到入侵防御相关问题，可参见 入侵防御 文档。

使用安全基线

最近更新时间：2024-04-22 17:25:32

本文档将为您介绍云防火墙安全基线的基本概念及运行流程，及如何通过云防火墙控制台使用安全基线功能，维护产品健康稳定。

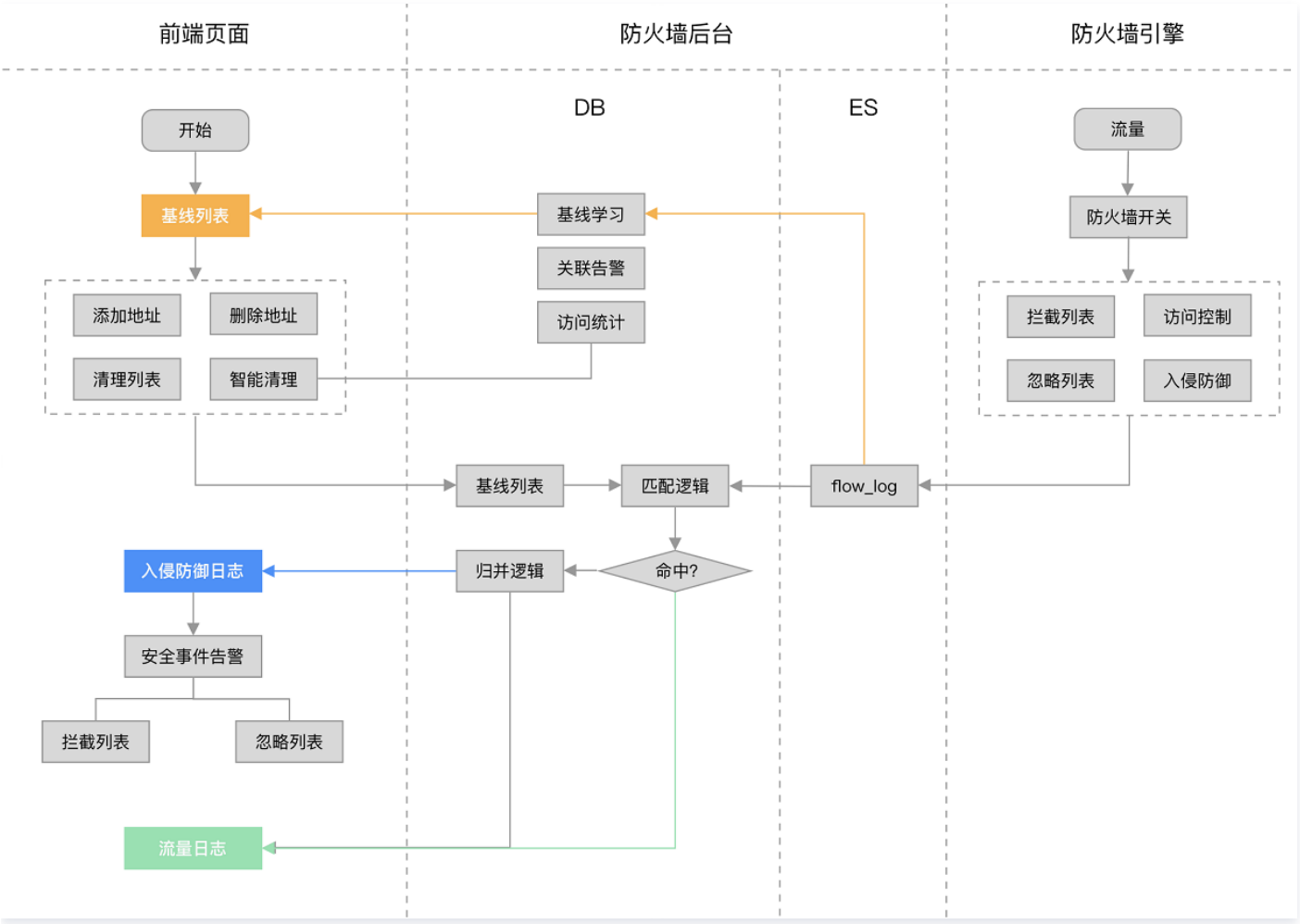
背景信息

什么是云防火墙的安全基线

安全基线指云防火墙通过观察一定时间范围内的流量访问情况，形成一个初步的 IP 地址或域名访问列表，用户可以根据安全评分、关联安全事件以及网络访问情况，通过添加或删除 IP 地址或域名，维护基线列表，从而形成最终的 **安全基线**。
当安全基线设置完成后，每新增一个在基线之外的 IP 地址或域名访问都会触发安全告警。用户可以在告警列表中对 IP 地址或域名进行处理，安全基线适用于重保期间的流量基线防护。

安全基线运行原理

安全基线运行原理如下图所示：



安全基线通过学习流量日志，结合访问情况并关联告警记录，生成初步的安全基线列表，用户可以在该基线列表中，通过智能清理，添加地址，删除地址和清空基线功能维护基线列表，提升基线评分，生成最终的 IP 访问白名单（即安全基线列表）。
安全基线建立完成后，后续访问的 IP 地址若属于安全基线内，则被判定为信任 IP，归并到日志审计的 流量日志 中。若在基线之外，将均被判定为恶意地址触发告警，归并到告警中心中，用户可以在 告警中心 的安全事件告警页面，将安全基线告警的 IP 地址进行“拦截”或“忽略”，完成安全事件处置。

前提条件

安全基线仅对旗舰版用户开放，请确保您 升级为旗舰版用户 后开始配置。

操作步骤

步骤1：配置安全基线规则

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到**安全基线模块**，单击**查看规则**，进入安全基线页面。

3. 首次进入安全基线页面，需配置安全基线规则。

字段说明：

- **开始时间**：安全基线开始流量观察的时间，单击“日历”，可自定义起始时间，最早可以选择30天之前的0点。
- **结束时间**：安全基线完成流量观察的时间，单击“日历”，可自定义终止时间，最晚可以选择30天之后的23:59:59。

> **注意：**
> 可分析时间范围从防火墙使用日期起至未来30天数据。

- **流量类型**：选择建立安全基线的流量方向。

> **说明：**
> 流量类型默认仅选择出站方向。如有特殊需求，请 提交工单 联系我们。

- **剔除资产**：被剔除资产下的相关流量，将不被计入安全基线的分析对象。

4. 单击**确认**，即可配置成功。

步骤2：执行安全基线学习任务

1. 在 配置安全基线规则 后，页面会自动开始执行基线学习，用户可以通过右下角查看基线学习进度。

> **说明：**
> - 后台会根据剔除后的资产进行基线学习，后续也仅针对基线内的资产触发警告。
> - 分析任务需要一定的时间（根据网络情况而定），可通过右下角任务状态查看进度。
> - 可单击**结束任务**，强制结束安全基线分析，并根据已分析列表作为安全基线。

2. 学习结束后，安全基线会根据用户所选时间范围对该时间段流量进行学习，提炼信息，为用户生成统计结果，并在当前页面下方建立一个访问详情列表。
   - **基线评分**：是根据列表中恶意 IP 地址占比，对当前访问环境进行的评估，为用户后续的安全基线维护提供参考指标，引导用户不断提升基线安全。
   - **访问详情列表**：则包含外部访问和主动外联两个方向的IP/域名。用户可以选择基线学习时间/基线检测时间来查看不同时间范围内的安全基线中的IP信息。
     - **基线学习时间**：加入基线时间到基线结束时间范围内的统计数据。
     - **基线检测时间**：加入基线时间到当前时间范围内的统计数据。

步骤3：编辑和维护安全基线

学习进程结束后，用户可以根据**基线评分**，通过智能清理，手动添加或删除来**提高**当前基线列表的**安全指数**，可通过如下两种方式维护安全基线：

- 用户可以在安全基线页面，通过单击**智能清理**或**添加地址**，自动或手动编辑安全基线列表。

- 在安全基线列表中，选择基线地址或域名，单击**清空基线**或者**删除**，来删除安全基线列表中的 IP 地址或域名。

下面将为您详细介绍如何使用 智能清理，添加地址，删除地址 和 清空基线 功能：

智能清理

一键清除基线列表中的恶意地址。云防火墙将自动对流量基线中的入侵防御告警进行关联统计，并将标有“未信任的”的恶意 IP 或域名从基线中删除，后续访问将触发警告。

> **注意：**
> 当外部访问和主动外联列表中，所有地址或域名均拥有**信任**标签后，**智能清理**功能将不能使用。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到**安全基线模块**，单击**查看规则**，进入安全基线页面。

3. 在“基线评分”模块，单击**智能清理**，将弹出“智能清理安全基线”弹窗。
4. 在“智能清理安全基线”弹窗中，选择系统监测到的基线类型以及 IP 数量。

5. 单击**确定**，系统将开始自动清除基线列表中，标有“未信任的”IP 或域名。

添加地址

自定义安全基线白名单，如果有特定的信任 IP 地址或域名，可以手动添加该 IP 地址或域名，将其加入安全基线列表中，则该 IP 后续访问将直接归入日志审计的 流量日志 中。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到**安全基线模块**，单击**查看规则**，进入安全基线页面。

3. 在“基线评分”模块，单击**添加地址**，将弹出“添加基线地址/域名”弹窗。
4. 在“添加基线地址/域名”弹窗中，选择将 IP 地址添加到全部、外部访问或主动外联的安全基线列表中，并手动输入信任的 IP 或域名。

> **说明：**
> 由于在配置安全基线规则时，流量类型 默认仅选择出站方向，因此基线类型仅支持选择“主动外联”，如有特殊需求，请 提交工单 联系我们。

- 全部：该地址将被同时加入外部访问和主动外联的安全基线列表中。
- 外部访问：该地址将只加入下方外部访问列表中。
- 主动外联：该地址将只加入下方主动外联列表中。

5. 单击**确定**，该 IP 将自动添加到所选基线类型列表中。

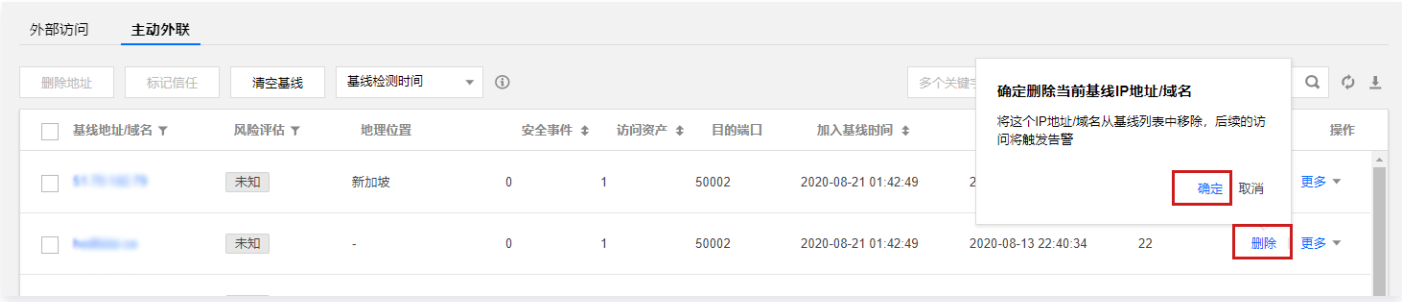
删除地址

用户可以直接在安全基线列表中，手动删除认为访问有异常的 IP 地址。如果后续需要恢复该地址，可以在 告警中心 中选择将该地址忽略，则地址又会回到基线列表中。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到**安全基线模块**，单击**查看规则**，进入安全基线页面。

3. 在安全基线页面下方，单击**外部访问**或**主动外联**。

4. 选择不信任的 IP 地址，在右侧操作栏，单击**删除**。



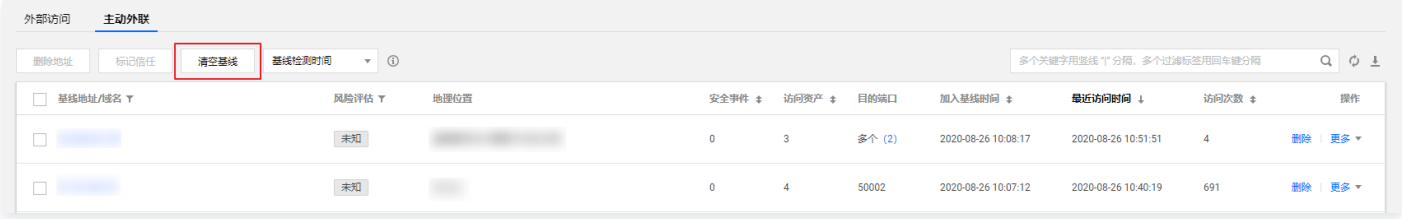
5. 在删除确认框中，单击**确定**，该 IP 地址将从安全基线列表中移除，后续该 IP 地址访问将会触发警告。

清空基线

如需停用安全基线功能，清除外部访问或主动外联列表中所有 IP 地址或域名，可使用清空基线功能，将清理掉所有安全基线内的 IP 地址和域名。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到**安全基线模块**，单击**查看规则**，进入安全基线页面。

3. 在安全基线页面下方，单击**外部访问**或**主动外联**。
4. 在列表上方，单击**清空基线**，将弹出确认弹窗。



5. 单击**确定**，则安全基线所有 IP 地址和域名将被清空，同时关闭警告基线开关。

> **注意：**
> 清空基线并不会删除日志中的原 IP 地址或域名记录，仅删除选中的安全基线列表。

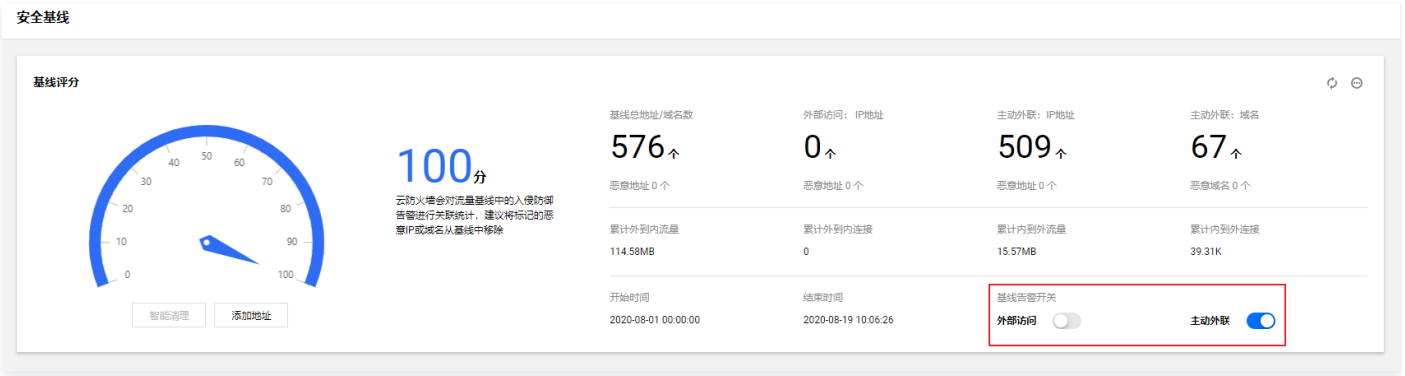
步骤4：启动安全基线管控

打开基线警告开关

安全基线建立完成后，用户需要打开基线告警开关，后续 IP 地址或域名访问，若不在安全基线中，将一律触发告警。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到**安全基线模块**，单击**查看规则**，进入安全基线页面。

3. 在“基线评分”模块，选择需要警告的流量方向。



- 开启**外部访问**时：针对入站方向流量，出现不属于基线内的访问时，将会触发安全告警。
- 开启**主动外联**时：针对出站方向流量，出现不属于基线内的访问时，将会触发安全告警。

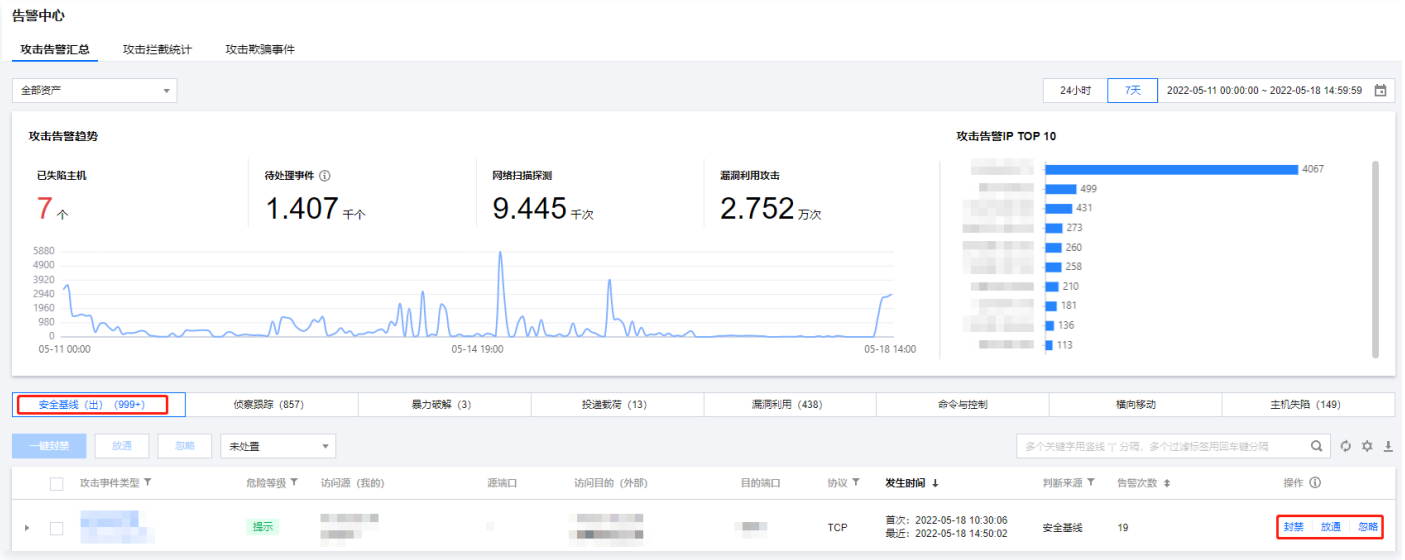
查看安全告警追溯流量记录

基线警告开关开启后，云防火墙将基于安全基线列表，将流量归为信任 IP 和不信任 IP 两类，分别归并到 流量日志 和 告警中心 中，用户可以在对应的页面查找相应的 IP 信息。

查看安全告警

1. 登录 云防火墙控制台，在左侧导航栏中，单击**告警中心**，进入告警中心页面。

2. 在攻击告警汇总页面中，单击**安全基线**，进入该页面，可以看到所有安全基线类型的告警信息，用户可以选择封禁、放通或者忽略，对该地址或域名进行处理。



- 单击**封禁**，则该 IP 地址将被加入封禁列表，后续访问将被阻断，可以在告警中心的攻击拦截统计页面中查看。
- 单击**放通**，则该 IP 将被加入基线列表，指定方向的访问将不再会经过安全基线的检测。
- 单击**忽略**，则该 IP 的告警事件将不会出现在告警列表和统计中，后续的流量也不会进行检测，可在列表中选择**已忽略**来查看被忽略的所有事件。

追溯流量记录

被列为安全基线内的 IP 或域名，可以在流量中心或流量日志中查询。

- 方式1： 登录 云防火墙控制台，在左侧导航栏中，选择**日志审计>流量日志**，查看入站流量或出站流量的 IP 或域名具体信息。
- 方式2：登录 云防火墙控制台，在左侧导航栏中，单击**流量中心**，查找已通过的 IP 或域名。

步骤5：重置安全基线（可选）

在基线建立一段时间后，如需更新基线列表，可以通过“重置安全基线”功能重新学习后续 IP 情况。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**，进入入侵防御页面。
2. 在入侵防御页面，找到**安全基线模块**，单击**查看规则**，进入安全基线页面。

3. 在“基线评分”模块，右上角选择 > **重置基线**，基线规则将被重置。

> **注意**
> 一旦重置基线，手动添加的地址以及手动添加标签将被清空。

4. 重置基线后，可根据需求重新配置安全基线规则，详情请参见 配置安全基线规则 。

管理防御操作

最近更新时间：2025-06-30 11:53:01

本文档将指导您通过入侵防御功能，识别访问控制规则以外的未知风险，并对公网 IP 的南北向流量进行入侵防御规则检测，同时避免云服务器中的漏洞暴露在互联网中。

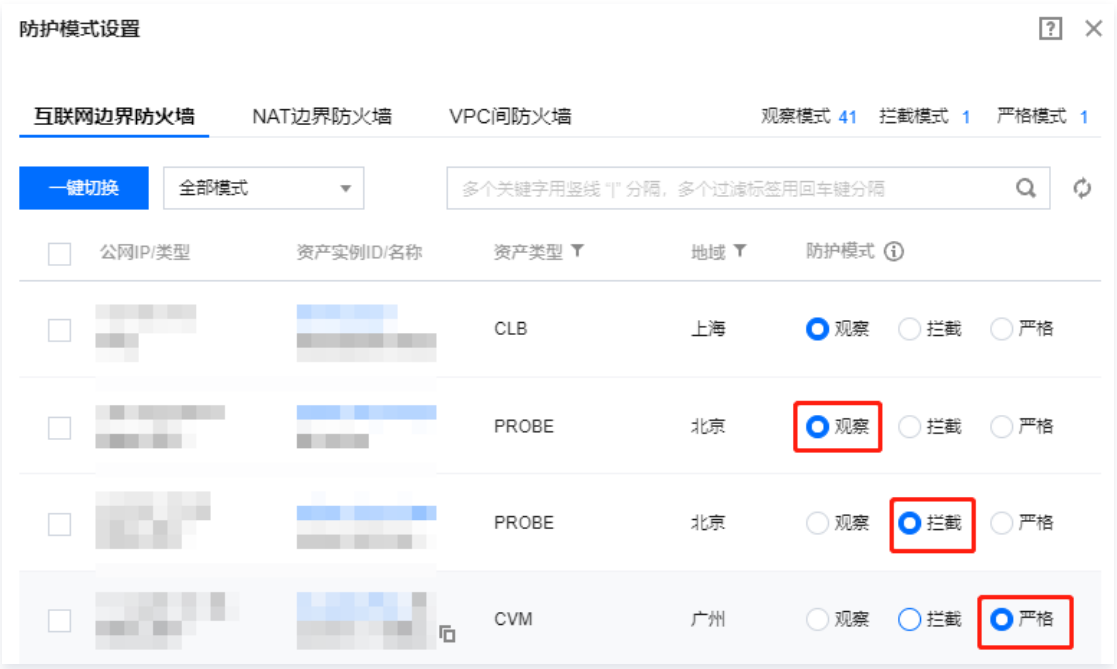
选择防护模式

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**。
2. 在入侵防御页面，找到“**防护模式**”模块，进行防护模式设置，防护模式共分为**观察模式**、**拦截模式**及**严格模式**三种模式。

> **说明：**
> 系统默认选择的防护模式是观察模式。

- 选择“观察模式”，威胁情报、基础防御、虚拟补丁均为检测模式，针对发现的恶意访问或网络攻击行为，只告警，不自动阻断连接。
- 选择“拦截模式”，自动拦截高置信度的网络攻击或恶意访问，威胁情报支持自动拦截出站恶意访问，基础防御支持自动拦截高置信度规则告警，虚拟补丁支持自动拦截所有被检测为漏洞利用的流量。
- 选择“严格模式”，威胁情报（出站域名威胁情报检测除外）、基础防御、虚拟补丁均为全局拦截模式，针对任何检测到的告警，自动阻断连接，可能产生误报，适用于重保或攻防场景。

3. 在防护模式右侧，单击**高级设置**，将进入高级设置弹窗。
4. 在高级设置弹窗中，用户在互联网边界、NAT 边界、VPC 间防火墙选择单个资产进行模式的更改，例如：部分资产可以设置为观察模式，部分资产为拦截模式，部分资产为严格模式。



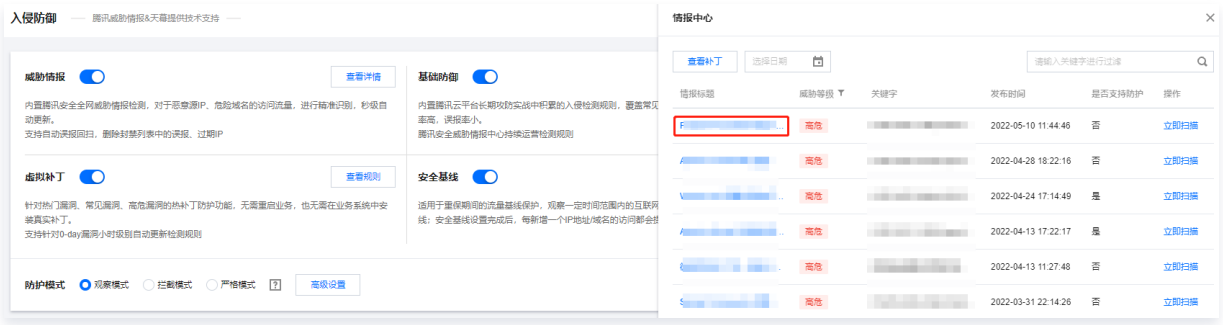
入侵防御功能说明

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**。
2. 在入侵防御页面右侧，可查看功能动态及功能说明：
   - **功能动态**：在功能动态模块，可查看入侵防御模块的功能。

   - **情报中心**：

     2.1.1 在功能动态右上方，单击**情报中心**，可查看安全威胁情报信息。

     2.1.2 在情报中心弹窗中，可单击具体的情报标题，在二级页面查看具体漏洞描述、威胁等级等具体信息。同时用户也可以针对具体的漏洞情报，使用扫描功能，检查自己的资产是否存在该威胁。



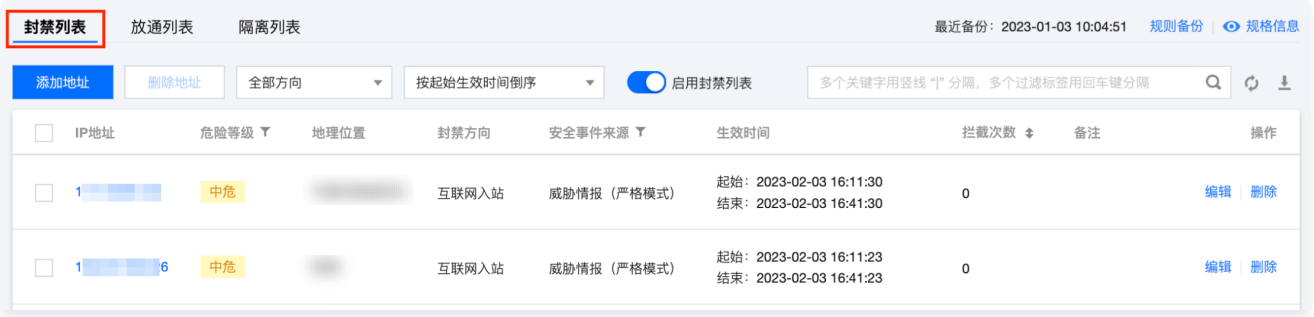
管理列表

1. 登录 云防火墙控制台，在左侧导航栏中，单击**入侵防御**。
2. 在入侵防御页面下方可查看“封禁列表”、“放通列表”和“隔离列表”。

封禁列表

查看封禁列表

1. 单击**封禁列表**，进入封禁列表页面。



2. 在封禁列表下，可以查看在 告警中心 > **攻击告警汇总**中，处置为“封禁”的IP及其相关信息，或者可以手动将IP添加进封禁列表。

停用封禁列表

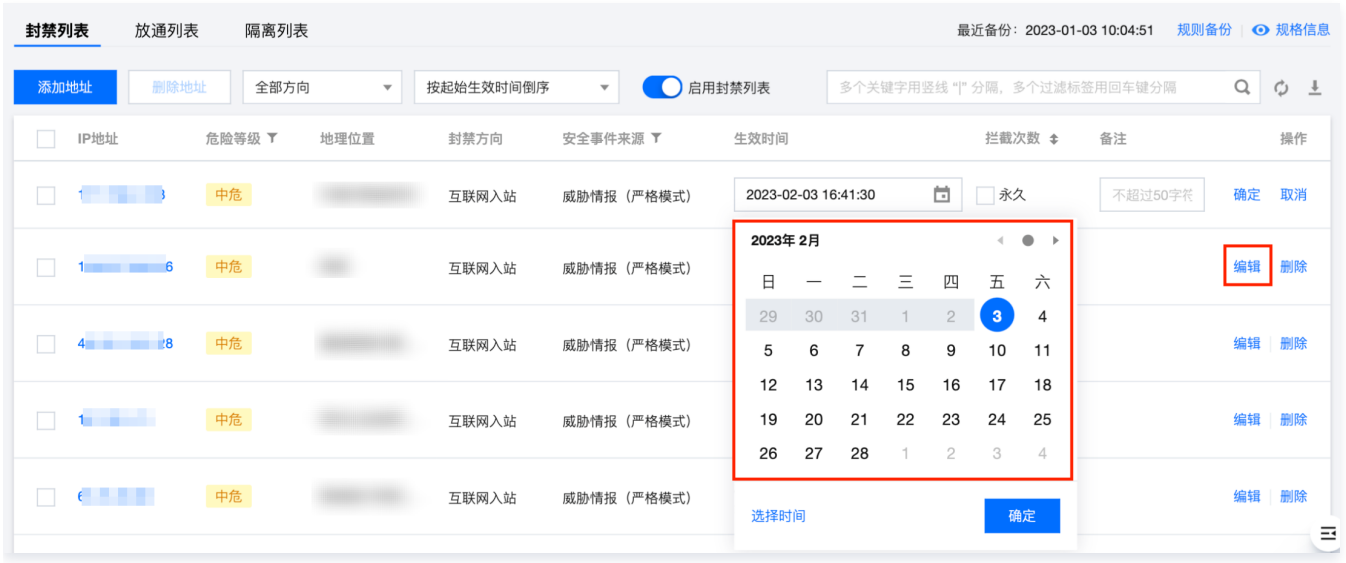
1. 当遇到紧急情况时，可单击 关闭“启用封禁列表”，将封禁列表停用，并进入 告警中心 > **攻击拦截统计**查看所有封禁统计，排查定位封禁来源。

2. 在定位并修复故障原因后，可单击 打开“启用封禁列表”开关，将该功能重新开启。

管理封禁列表的生效时间

在封禁列表内，当某一个 IP 的生效时间到期后，列表会自动删除该 IP，此时该 IP 后续的流量访问将不会被防火墙封禁。因此，为了避免黑名单自动移除存在安全隐患的 IP，可以在列表右侧操作栏，单击**编辑**，对需要操作的 IP 的终止时间和日期进行修改。

> **说明：**
> 位于封禁列表内的 IP 地址，会按照出站或入站方向阻断所有经过云防火墙的流量，并记录在**日志审计**>** 入侵防御日志 **内。



管理封禁列表规格信息

1. 单击**规格信息**，即可查看当前提供的总列表配额以及剩余配额信息。

2. 当剩余配额不足时，可单击**升级扩容**，购买封禁列表配额。

白名单策略

查看白名单策略

1. 在入侵防御页面，单击**白名单策略**，进入白名单管理页面。

2. 在白名单策略页签中，可以看到在 告警中心 > **攻击告警汇总**中，处置为放通的 IP 及其相关信息，或者可以手动添加地址到白名单列表。

> **注意：**
> - 白名单列表中的 IP 地址，会直接绕过 IDPS 功能。
> - 封禁列表和白名单策略有规则数量上限，黑白名单数量上限相同。
> - 各版本数量上限请参见 购买指南 。

新增白名单策略

在入侵防御页面，单击**添加策略**，选择**加白类型**，配置相关参数，单击**添加**。

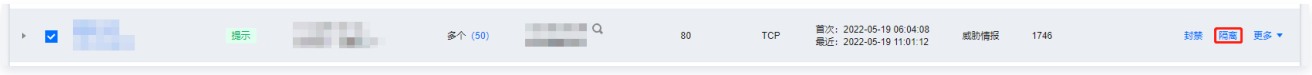
加白类型	说明
IP 地址	针对公网访问或内网访问基于 IP 地址匹配定向放行流量。
资产实例	针对内网方向基于资产实例匹配定向放行流量。
域名	针对公网出向或内网出向基于访问域名匹配定向放行流量。
威胁情报地址	添加后将不再匹配情报类型告警，严格模式下不会自动拉黑这些 IP，但基础防御规则继续生效。
自定义策略	针对特定访问源、访问目的、入侵防御规则精准匹配定向放行流量。 • 如果需要下发至互联网边界防火墙，访问源和访问目的均需要填写公网 IP。 • 如果需要下发至NAT边界防火墙，访问源和访问目的需要一个为公网IP另一个为内网 IP。 • 如果需要下发至 VPC 间防火墙，访问源和访问目的均需要填写内网 IP。 • 若所选入侵防御规则的生效范围与下发策略的生效范围不一致将不会命中。 • 自定义策略最多支持添加 10 条，如果更多需求请提交工单评估。

隔离列表

查看隔离列表

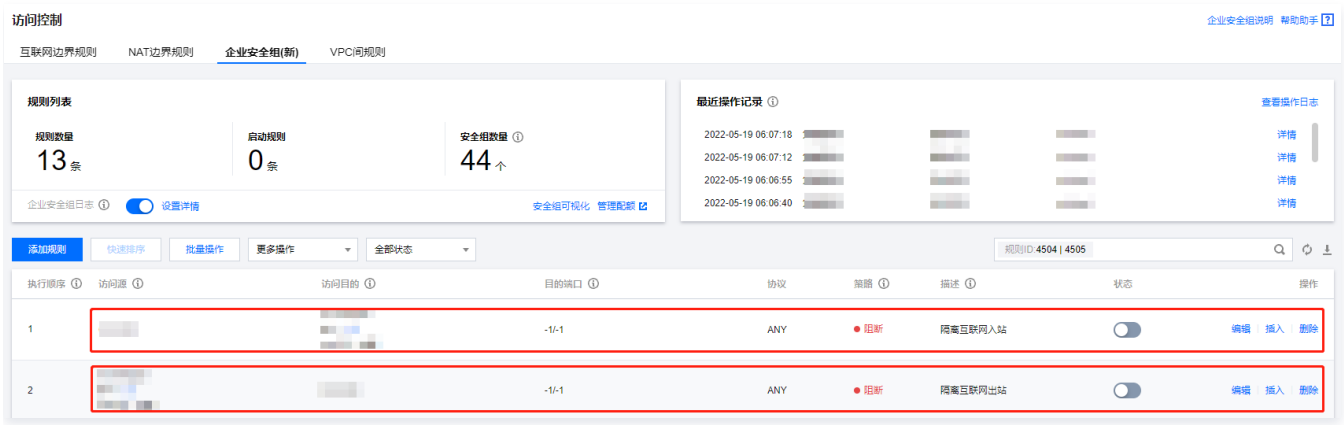
1. 单击**隔离列表**，进入隔离列表页面。

2. 在隔离列表中，可以看到在 告警中心 > 攻击告警汇总 > 主机失陷中，处置为隔离的 IP 及其相关信息。



查看规则

失陷主机 IP 的隔离是通过安全组来实现的，单击**查看规则**，可以跳转到企业安全组页面，查看详细的规则信息。

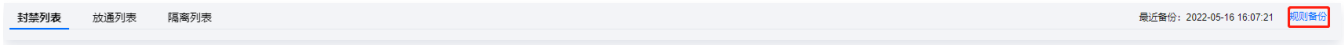


管理隔离列表的生效时间

在隔离列表内，当某一个 IP 的生效时间到期后，列表会自动删除该 IP，此时该 IP 的安全组规则也会被删除。因此，为了避免已失陷的 IP 被自动移出隔离名单，可以在列表右侧操作栏，单击**编辑**，对需要操作的 IP 的终止时间和日期进行修改。

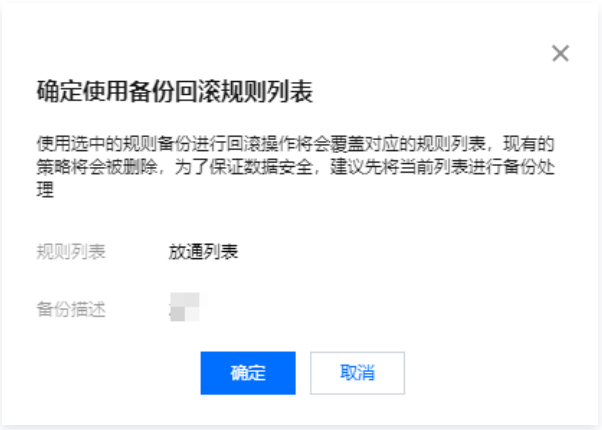
策略备份与回滚

单击**规则备份**，即可将现有的封禁列表和放通列表规则进行备份，同时当规则发生了很大的变化之后，单击备份文件右侧的**回滚**，即可将规则进行复原。



1. 在策略备份与回滚页面，单击**新增备份**，在旁边的下拉框选择封禁列表或者是放通列表，输入描述，单击**确定**，完成规则备份。

2. 规则回滚，单击备份列表最右侧的**回滚**，将规则进行还原。



相关信息

如遇到入侵防御相关问题，可参见 入侵防御 文档。

全流量检测与响应

最近更新时间：2025-07-01 16:12:12

云防火墙全流量检测与响应 NDR 是一个云原生网络检测与响应功能。全流量检测与响应功能可以实时收集、存储和分析网络中的全部流量数据，发现网络攻击威胁，还原传输文件提高网络安全性。

> ⚠ 注意：
> 提交工单 申请试用全流量检测与响应 NDR 功能。

应用场景

云上流量全审计、网络安全监控、针对 APT 等高级威胁分析。

技术方案

通过旁路镜像网络流量，进行异步检测，对业务流量无影响；特殊场景下也支持 Agent 终端采集模式检测流量。

模式	说明
流量镜像模式	使用弹性网卡镜像流量至防火墙集群进行分析，对业务无影响，消耗服务器内网带宽。
终端采集模式	在服务器上安装终端探针采集流量，消耗 CPU 性能以及内网带宽。 • 支持操作系统类型：Tlinux、Ubuntu、centos（内核版本3.2以上）。 • 需安装自动化助手，操作详情请参见 安装自动化助手客户端 。

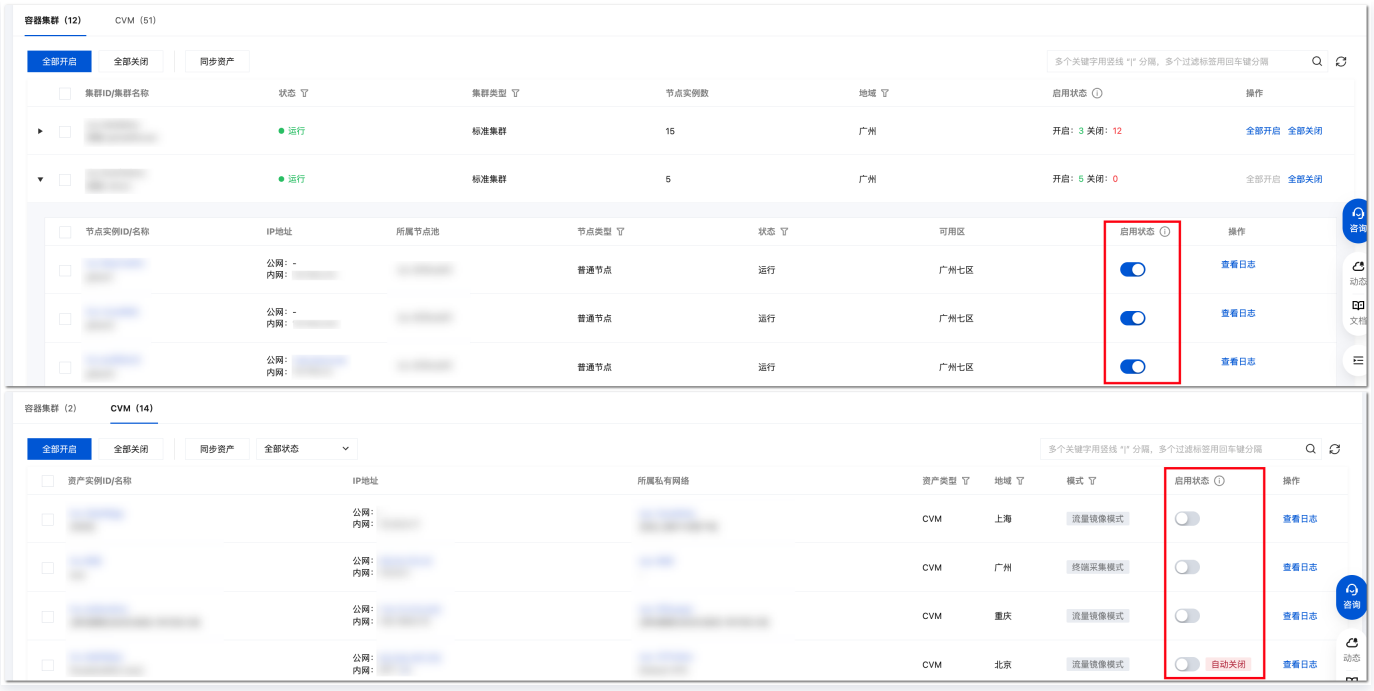
使用教程

1. 登录 云防火墙控制台，在左侧导航栏中，单击**全流量检测与响应**。

   > ⚠ 注意：
   > 提交工单 申请试用全流量检测与响应 NDR 功能。

2. 在全流量检测与响应页面，容器集群支持根据节点启用全流量检测与响应分析开关，CVM 支持根据资产启用全流量检测与响应分析开关。

   开启全流量检测与响应分析开关后，云防火墙会镜像出/入服务器流量进行以下分析：
   - 所有流量会经过入侵防御引擎，基于入侵防御规则进行检测分析并告警。
   - 日志记录所有进出服务器的流量，包括数据包头（Header）、有效载荷（Payload）。其中对于非加密流量，会对 Payload 进行分析解读，还原协议与应用，每个报文最大记录1000字节。



3. 在全流量检测与响应页面，单击右上角的**全流量检测与响应设置**，支持新资产流量解析设置、全流量检测与响应带宽设置及全流量检测与响应超量处置设置。
   - 新资产流量解析设置：支持设置新资产是否自动开启流量解析。
     a. 资产类型设置为**全部新资产**时
        - 自动开启流量解析开关**开启时**，发现新资产（公网资产与非公网资产）后会自动开启流量解析。
        - 自动开启流量解析开关**关闭时**，发现新资产（公网资产与非公网资产）后不会自动开启流量解析。

     b. 资产类型设置为**仅新公网资产**时
        - 自动开启流量解析开关**开启时**，发现新公网资产后会自动开启流量解析，非公网资产不会自动开启流量解析。
        - 自动开启流量解析开关**关闭时**，发现新资产（公网资产与非公网资产）后不会自动开启流量解析。
   - 全流量检测与响应带宽设置

     a. 总流量 = 各实例的出入流量峰值之和，请确保流量分析带宽或弹性分析带宽大于总流量。

     b. 弹性防护：支持设置弹性分析带宽，当流量小于弹性分析带宽时进行分析，当流量大于弹性分析带宽时，进行超量处置。
   - 全流量检测与响应超量处置：流量分析带宽超量不会导致客户业务流量丢包或影响流量速率，但将无法提供全流量检测与响应功能。

     a. 带宽规格超量限流与恢复机制
        - 权重范围：0 – 100（默认 50），值越大优先级越高。
        - 限流机制：实时带宽 > 购买规格时，系统优先自动关闭高权重解析（权重相同则按峰值带宽降序关闭），直至实时带宽降至购买规格内。
        - 恢复机制：实时带宽 ≤ 购买规格时，系统优先自动开启高权重解析（权重相同则按峰值带宽降序开启），自动开启全流量检测与响应开关。

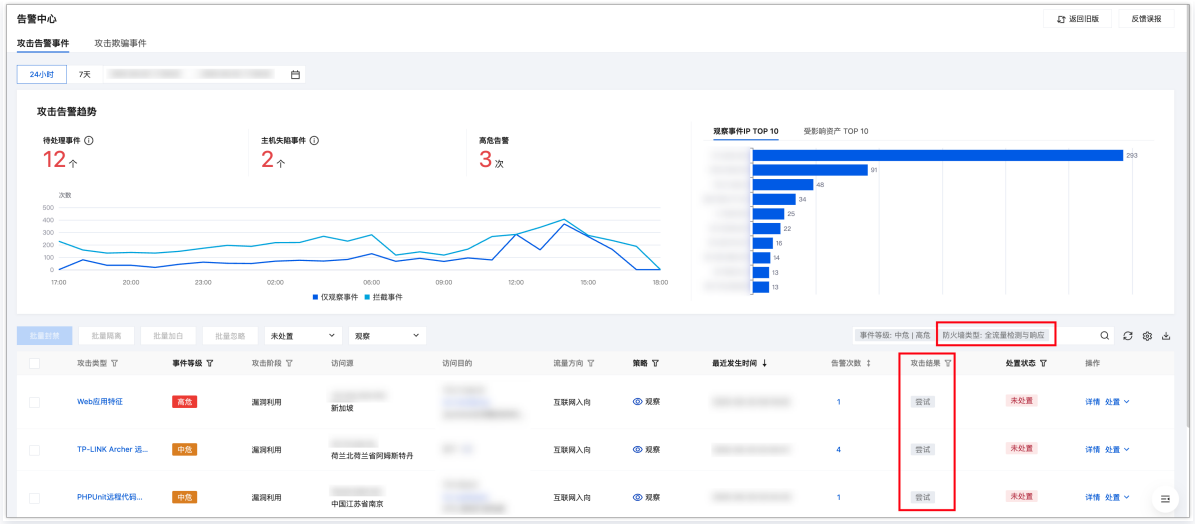
     b. 单机带宽过载自保护与恢复机制
        - 冷却时间：30 – 1440 分钟（默认 60 分钟），支持自定义配置。
        - 自保护机制：每隔30s检测服务器带宽使用率，当服务器带宽使用率 > 40%（因镜像流量，对应总带宽使用率 > 80%），系统关闭该服务器全流量检测与响应开关。
        - 恢复机制：每隔30s检测服务器带宽使用率，当服务器带宽使用率在冷却时间的最后2分钟内均 ≤ 40%，系统自动开启全流量检测与响应开关。

     c. 支持批量编辑权重。

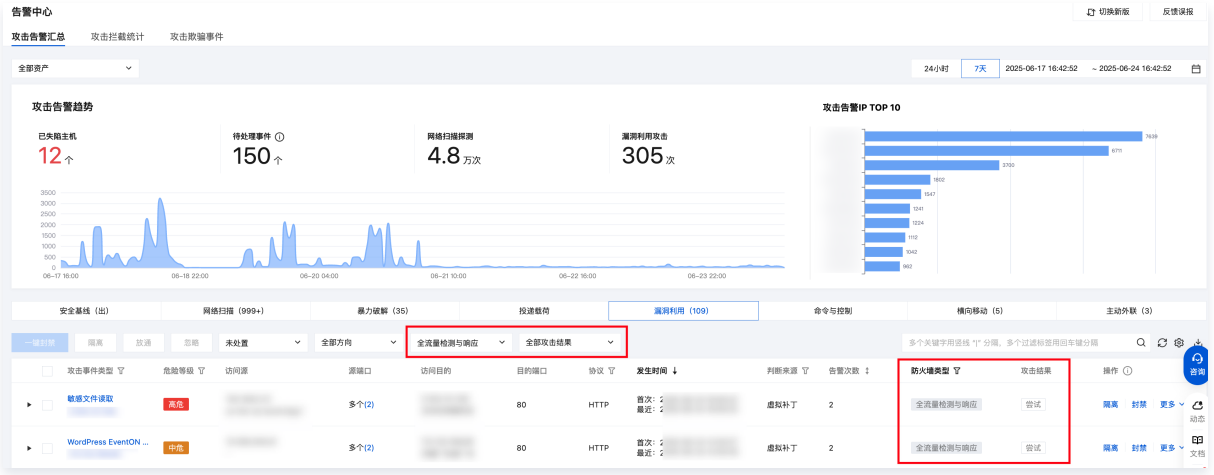
     d. 带宽规格超量会进行系统横幅提醒，超量告警及超量处置均会发送站内信、邮件、短信等通知。

版权所有：腾讯云计算（北京）有限责任公司

- 在 告警中心页面，查看全流量检测与响应中发现的威胁告警，支持分析检测横向移动、主动外联等八类告警，支持攻击结果判定。
  - 新版告警中心



○ 旧版告警中心



4. 在 日志审计 > 全流量检测与响应日志页面，可查看全流量检测与响应流量分析日志、流量告警日志、检出文件列表等信息。

资源说明

全流量检测与响应 NDR 公开测试期间，可申请测试资源如下：

功能指标	测试资源性能	备注
单用户最大资产接入数量	100台服务器	支持 提交工单 申请增加。
单机器最大接入流量	1Gbps	支持 提交工单 申请增加，连续3分钟超过测试资源性能100%将关闭该机器流量采集开关不再分析，其他机器开关不处置，该过程对业务流量无影响。
单用户总带宽	20Gbps	支持 提交工单 申请增加，连续3分钟超过测试资源性能120%将关闭流量采集开关不再分析，该过程对业务流量无影响。

全流量检测与响应带宽超量与恢复机制说明

流量分析带宽超量不会导致客户业务流量丢包或影响流量速率，但将无法提供全流量检测与响应功能。

带宽规格超量限流与恢复机制

- 权重范围：0 – 100（默认 50），值越大优先级越高。
- 限流机制：实时带宽 > 购买规格时，系统优先自动关闭高权重解析（权重相同则按峰值带宽降序关闭），直至实时带宽降至购买规格内。
- 恢复机制：实时带宽 ≤ 购买规格时，系统优先自动开启高权重解析（权重相同则按峰值带宽降序开启），自动开启全流量检测与响应开关。

单机带宽过载自保护与恢复机制

- 冷却时间：30 – 1440 分钟（默认 60 分钟），支持自定义配置。
- 自保护机制：每隔30s检测服务器带宽使用率，当服务器带宽使用率 > 40%（因镜像流量，对应总带宽使用率 > 80%），系统关闭该服务器全流量检测与响应开关。
- 恢复机制：每隔30s检测服务器带宽使用率，当服务器带宽使用率在冷却时间的最后2分钟内均 ≤ 40%，系统自动开启全流量检测与响应开关。

版权所有：腾讯云计算（北京）有限责任公司

零信任运维
概述

最近更新时间：2024-04-24 09:52:51

企业在日常运维过程中，往往会面临需要从办公网访问生产网的服务器、数据库、内部 OA 系统等场景，如何安全高效运维是企业一直在尝试解决的难题。当 SSH、RDP、内部 OA 系统以及数据库公网 IP 等资产直接暴露在互联网中，由此带来的攻击现象在重保期间尤其明显，因此云防火墙对上述场景提供了基于零信任的安全运维方案。

模块概览

零信任运维的使用，按照事前接入资产和身份、事中权限配置、事后审计的使用思路可以分为四个模块，分别是接入管理、资产管理、权限管理和零信任运维日志。

- 接入管理：负责创建零信任运维实例并接入运维资产的网络、接入iOA或微信的身份体系、接入 Web 服务的网站域名等准备工作。
- 资产管理：负责服务器资产、Web服务资产、数据库资产的运维配置，包括服务器登录账密、Web 服务端口及接入域名等相关配置工作。
- 权限管理：负责根据已接入的身份体系及运维资产，按照人和资产的维度分配运维权限，支持身份视角或规则视角添加权限。

使用零信任防护

1. 零信任运维支持基于 iOA 的内网有端运维，可通过 iOA 身份免密对云上资源进行访问控制，详情可参考 通过 iOA 进行有端运维 。
2. 零信任运维支持基于微信或 iOA 的公网无端运维，可通过微信或 iOA 扫码的方式对云上资源进行访问控制，详情可参考 通过微信或 iOA 进行无端运维 。

日志

零信任运维日志

零信任运维日志 可按照资产维度分别展示服务器、Web 服务、数据库中的访问情况，对登录成功或非法访问等日志进行审计和分析，支持操作回放。

零信任运维操作日志

在 操作日志页面，选择**零信任运维操作**，即可查看零信任防护功能的操作详情和对应账号。

版本说明

云防火墙零信任运维功能需额外付费购买，具体计费及规格信息可参见 购买指南 。

版权所有：腾讯云计算（北京）有限责任公司

实践教程
通过 iOA 进行有端运维

最近更新时间：2024-04-23 15:18:21

背景信息

在线下的办公网访问云上的生产网一是个网络隔离和权限管控的难题，如何最小化安全风险的同时提升日常的运维体验，是每个企业都企图解决的痛点。现在通过 iOA 零信任安全管理系统与云防火墙联合使用，避免了云上与线下复杂的网络打通和配置，实现了即开即用的便捷接入体验，并且同时支持基于身份的访问控制和审计。

概述

有端运维需要用户客户端设备登录 iOA 账号，受控资产支持服务器、Web 服务和数据库。

步骤一：接入准备工作

前提条件

请确认您已在 iOA 控制台完成了相关功能的配置，详情请参见 远程接入-开箱指引 。

步骤1：启用零信任运维实例

零信任运维实例（以下简称运维实例）负责提供整合 iOA 的连接器与零信任网关通信，打通资产与运维实例之间的网络通信。在启用运维实例之前，您需要先根据购买的配额及资产所属地域进行规划，确认需要开启的运维实例所在地域。确定地域后，详情请参见 启用零信任运维实例 。

> ⚠ **注意：**
> 使用 iOA 有端运维请务必绑定运维 IP，否则将无法使用所有有端运维功能。

步骤2：接入资产网络

在启用零信任运维实例后，还需要将实例与资产之间的网络打通以实现网络流向的匹配。云防火墙提供以 VPC 粒度进行接入的快捷操作，仅需开启对应地域下的 VPC 开关即可完成接入，详情请参见 以 VPC 粒度进行资产接入 。

> ⚠ **注意：**
> 由于实例规格限制，每个实例仅支持接入9个 VPC。

步骤3：接入身份信息

至此您已完成了基本的网络打通，现在您需要接入需要运维的身份信息。请您根据需要导入 iOA 组织目录，详情请参见 身份接入 。

> ⚠ **注意：**
> iOA 目录接入仅支持以组织维度进行接入，接入后不会默认分配权限，请放心操作。

步骤二：资产配置工作

在接入准备工作中，您已经完成了网络的打通、身份的接入，接下来您需要对接入的资产配置相关运维参数。

服务器类型资产

服务器类型资产支持 Linux 及 Windows 的远程运维，默认运维端口为22和3389，如果您需要修改运维端口请参考 配置运维端口 。
服务器支持托管服务器的密码密钥，从而避免密码密钥从员工泄露，实现基于身份的免密登录，详情请参考 密码密钥托管 。

> ⚠ **注意：**
> 资产列表中，仅限在前述接入资产网络中启用了 VPC 下的资产才可进行远程运维。

Web 服务类型资产

如果您需要通过公网来运维 OA 等 Web 类业务，可以先手动添加 Web 服务，详情请参见 添加 Web 服务 。

版权所有：腾讯云计算（北京）有限责任公司

> **注意：**
> Web 服务添加后无需绑定域名即可使用内网有端运维，请使用真实服务地址访问即可。

数据库类型资产

数据库资产会自动拉取云上您拥有的相关 PaaS 服务，现有支持类型包括 MySQL、MariaDB、Redis、CKafka、ElasticSearch 五种数据库类型。您可以根据情况点击同步资产重新拉取数据库资产进行同步，详情请参见 数据库管理 。

> **说明：**
> 云防火墙无需配置数据库运维信息，所有信息以对应产品控制台为准，配置权限后可直接通过数据库地址进行连接。

步骤三：权限配置工作

权限本质上就是基于身份和资产的三元组白名单，因此无论是从权限规则本身的视角，还是资产视角，或是身份视角，都可以对权限进行管理和添加。

- 从权限规则本身的视角进行权限管理或者添加权限，详情请参见 规则视角 。
- 从身份的视角对拥有权限的资产进行管理或编辑，详情请参见 身份视角 。
- 从资产的视角对拥有权限的用户或组织进行管理或编辑，请前往各个资产类型的管理页面。

步骤四：验证登录是否正常

通过 iOA 进行有端运维您可以参考 iOA 用户内网访问运维资产 。

通过微信或 iOA 进行无端运维

最近更新时间：2024-04-24 09:31:01

背景信息

近来云上Web攻击、挖矿、勒索等安全事件猖獗，腾讯安全工程师从大量安全工单反馈中，跟进溯源分析发现多数用户存在较多边缘业务网站或内部 OA 等核心业务网站错误地开放到公网，导致网站被渗透；且由于后端服务器将22、3389远程运维端口直接暴露在互联网中，同时使用了强度较弱的登录口令，导致云服务器很容易被暴力破解登录，影响业务稳定性甚至系统崩溃。
在云上，22和3389端口是仅次于80、443和8080的第四大流量端口，同时也是远程运维和登录的重要端口。在此之前，用户可以通过在云防火墙中设置 IP 地址白名单的访问控制策略，来限制外部对其重要端口的访问。但是由于非职场办公已成为新常态，基于 IP 地址的白名单无法应对远程办公和运维的场景，因此腾讯云防火墙设计了基于身份的访问控制功能，通过微信扫码认证或 iOA 体系鉴权的形式管控 Web 网站和云服务器的远程登录，从源头上避免服务器被暴破登录。

概述

无端运维当前针对的防护资产有两类：服务器和 Web 服务。

功能简介

云防火墙零信任运维支持基于微信或 iOA 认证实现远程访问，涵盖公网或内网 Web 服务、 SSH 和 RDP 两类协议所代表的服务器等。
运维资产防护方案：

- 该功能解决了传统静态 IP 白名单安全策略不适用于远程办公场景下的 IP 变动问题，也规避了云服务器运维端口被暴破或撞库的风险。云防火墙零信任运维功能无需部署实例和代理，也无需装客户端（iOA 身份可能需要安装客户端），实现“零部署、免代理、无客户端”的畅快体验。

Web 的防护方案提供了基础防护和高级防护两种防护模式。其中：

- 基础防护：自动过滤人机、攻击者，对于没有购买 WAF 的用户，可以使用该功能对 Web 业务进行防护。
- 高级防护：微信扫码或 iOA 认证，对 HTTPS 加密协议的 Web 服务增加了身份的访问控制，所有访问网络服务的用户都需要验证身份，重要时期保护、防渗透推荐功能。

Web 服务管理，可用于应对0day 漏洞和网络攻击，可以使用 Web 防护对企业的 OA 系统、邮件系统、企业 VPN、后台等关键系统进行防护，支持保护内网、公网、IP 型和域名型 Web 服务。

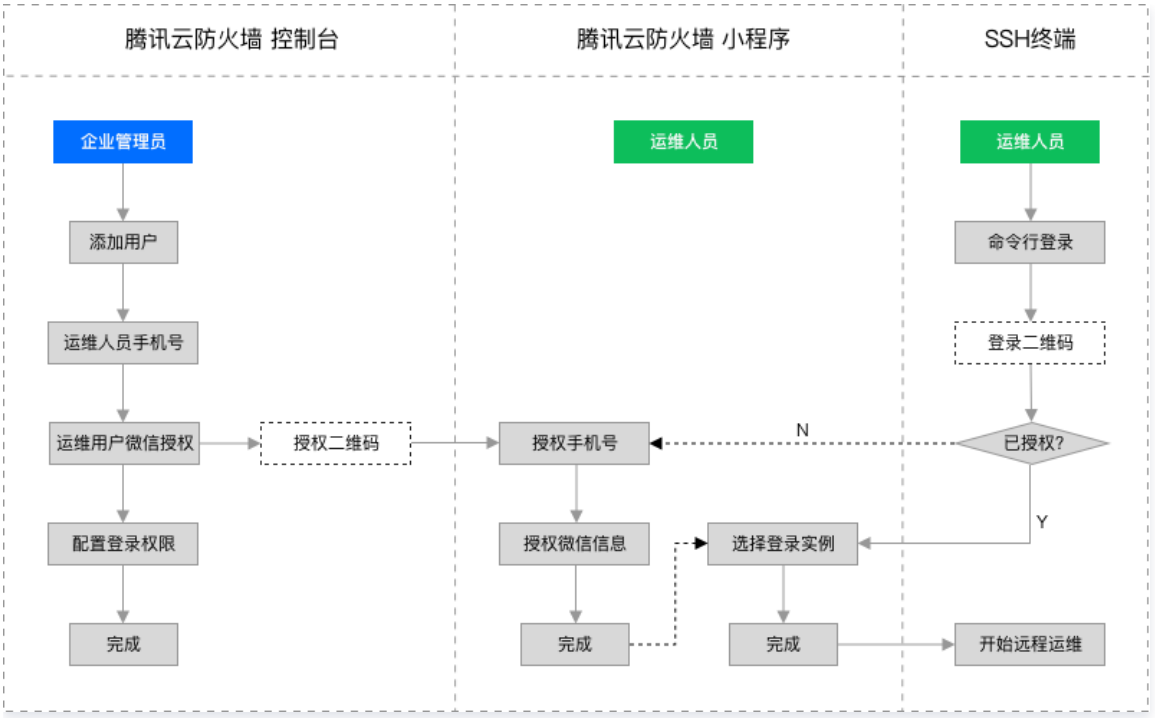
功能特点

- 基于零信任原理，支持基于微信或 iOA 快捷认证，安全便捷。
- 可在互联网边界，屏蔽管理端口，隐匿源站。
- 零部署、免代理、无客户端。
- 自动过滤 Web 攻击、漏洞利用攻击；避免暴破和撞库。
- 微信内访问 Web 服务免扫码，一键认证。
- 全流程、全用户审计，自动记录登录日志。

功能流程

云防火墙零信任运维的系统使用大体可以分为接入准备、资产配置、权限配置、登录验证四个流程。以微信身份 SSH 登录服务器运维举例，以下为流程概览：

版权所有：腾讯云计算（北京）有限责任公司



步骤一：接入准备工作

接入准备工作可以分为四个环节，分别是启用零信任运维实例、接入资产网络、接入身份信息、接入 Web 域名。

步骤1：启用零信任运维实例

零信任运维实例（以下简称运维实例）负责提供公网反代并打通与资产之间的网络通信，在启用运维实例之前，您需要先根据购买的配额及资产所属地域进行规划，确认需要开启的运维实例所在地域。确定地域后，可参见 启用零信任运维实例 。

> **注意：**
> 如果您仅需要运维公网资产，您无需绑定运维 IP 即可通过公共域名 `cfw.tencentcs.com` 进行运维；如果您需要运维内网资产请绑定运维 IP。

步骤2：接入资产网络

在启用零信任运维实例后，还需要将实例与资产之间的网络打通以实现反向代理。云防火墙提供以 VPC 粒度进行接入的快捷操作，仅需开启对应地域下的 VPC 开关即可完成接入，详情请参见 以 VPC 粒度进行资产接入 。

> **注意：**
> 由于实例规格限制，每个实例仅支持接入9个VPC。

步骤3：接入身份信息

至此您已完成了基本的网络打通，现在您需要接入需要运维的身份信息。公网的无端运维仅支持微信身份，您也可以通过登录页面回调至 iOA 进行有端授权访问。现在请您根据需要，选择接入微信身份或导入 iOA 组织目录，详情请参见 身份接入 。

> **注意：**
> 微信身份通过手机号关联，请确保添加的微信账号关联正确的手机号码。

步骤4：配置访问域名

域名访问在无端公网运维中是必要的，因为公网的无端运维需要由防火墙的零信任运维实例提供反向代理，并通过域名访问。如果您需要使用此功能，请务必接入域名。
域名分为运维域名和 Web 域名，运维域名主要负责服务器的远程运维，Web 域名主要负责 Web 服务的反代访问。接入方法请参见 域名接入 。

> **注意：**

请确保接入的域名已备案，否则可能会被腾讯云拦截正常访问。

步骤二：资产配置工作

在接入准备工作中，您已经完成了网络的打通、身份的接入、域名的接入，接下来您需要对接入的资产配置相关运维参数。

服务器类型资产

服务器类型资产支持 Linux 及 Windows 的远程运维，默认运维端口为22和3389，如果您需要修改运维端口请参见 配置运维端口 。
服务器支持托管服务器的密码密钥，从而避免密码密钥从员工泄露，实现基于身份的免密登录，详情请参见 密码密钥托管 。

注意：
资产列表中，仅限在前述接入资产网络中启用了 VPC 下的资产才可进行远程运维。

Web 服务类型资产

如果您需要通过公网来运维OA等Web类业务，可以先手动添加 Web 服务，详情请参见 添加 Web 服务 。
添加完成后，如果需要通过公网来进行运维，请务必进行域名绑定，域名绑定详情请参见 绑定域名 。

注意：
- 当前步骤强依赖接入准备工作，请确保已完成实例的启用、资产的接入、域名及证书的托管。
- 绑定域名建议采用高级防护方案，以方便配置基于身份的访问控制规则。

步骤三：权限配置工作

权限本质上就是基于身份和资产的三元组白名单，因此无论是从权限规则本身的视角，还是资产视角，或是身份视角，都可以对权限进行管理和添加。
- 从权限规则本身的视角进行权限管理或者添加权限，详情请参见 规则视角 。
- 从身份的视角对拥有权限的资产进行管理或编辑，详情请参见 身份视角 。
- 从资产的视角对拥有权限的用户或组织进行管理或编辑，请前往各个资产类型的管理页面。

步骤四：验证登录是否正常

- 服务器类型资产的登录您可以参考 微信用户公网远程登录服务器 。
- Web 服务类型资产的访问您可以参考 微信或 iOA 用户公网访问 Web 服务 。

版权所有：腾讯云计算（北京）有限责任公司

接入管理

概述

最近更新时间：2024-04-22 17:25:33

接入管理模块主要负责使用零信任运维的前期准备工作，包含零信任运维实例的创建、运维资产 VPC 网络的接入、iOA 身份及微信身份的接入、公网运维域名及 Web 服务域名的接入。

操作步骤

云防火墙通过在每个地域创建一个零信任运维实例，负责打通到对应运维资产所在VPC的网络通信。

1. 您需要在 实例管理 模块中，在启用对应地域的运维实例开关。
2. 您需要在 资产接入 模块中，接入上一步已开启地域运维实例下的 VPC 网络。
3. 您需要在 身份接入 模块中，接入包含运维人员的身份体系，可通过 iOA 导入或微信添加。
4. 如果您需要使用公网运维，您需要在 域名接入 中接入公网运维域名或公网 Web 服务域名。

版权所有：腾讯云计算（北京）有限责任公司

实例管理

最近更新时间：2024-04-22 17:25:33

1. 登录 云防火墙控制台，在左侧导航中，选择**零信任运维 > 接入管理**。
2. 在实例管理页面中，您可以完成对零信任运维实例的管理，方便后续进行资产接入和运维。

启用零信任运维实例

当前版本每个地域对应1个零信任运维实例，您可以根据您拥有的配额选择是否启用指定地域的实例开关。

1. 找到所需运维资产所在的地域，单击右侧的 用当前地域运维实例。

> **说明：**
> 如果列表中没有您资产所在地域，请前往 资产中心 单击**资产更新**。

2. 如果您暂未绑定运维 IP，则当前地域下资产仅支持通过公共域名运维公网资产，不支持 iOA 认证，不支持内网资产的运维。

> **说明：**
> 如何接入公网运维域名请参考 域名接入 。

3. 如果您已经绑定了运维 IP，则开启开关后，当前地域同时支持公网资产和内网资产的运维，您可以使用 iOA 身份或微信身份配置访问控制权限。

4. 完成启用后，您可以前往 资产接入 进行下一步的操作。

> **说明：**
> 启用零信任运维实例后，当前地域实例下的资产不会立即接入零信任网络，您需要前往 资产接入 手动选择需要接入的 VPC 网络。

绑定运维 IP

绑定运维 IP 可以让零信任运维实例具备公网访问及与 iOA 网关通信的能力，故可以支持基于 iOA 的身份访问控制，还可以支持对应实例下的内网资产的远程运维。

1. 找到所需运维资产所在的地域，单击下方的运维 IP 右侧的。

2. 您可以从现有闲置 EIP 中选择一个或新建一个 EIP 绑定至当前实例，单击**保存**后即可生效。

> **说明：**
> 在地域实例开关未开启状态下，选择运维 IP 并不会将 EIP 立即绑定至实例，**可能会产生一定闲置费用**。请绑定完成后尽快启用开关或在地域实例开启状态下绑定 EIP。如您已确定不再使用此实例，请将 EIP 绑定关系调整为暂不选择。

3. 单击运维 IP-2 右侧的，可以绑定多个运维 IP。

> **说明：**
> 当前版本最多可支持绑定2个运维 IP，可实现实例的高可用和动态负载均衡，绑定第二个运维 IP 需要购买零信任运维高级版。

查询零信任运维实例配额

在 接入管理 的规格信息中，可以查看已授权的运维实例数量和剩余配额。

零信任运维
查看指引
接入管理
资产管理
权限管理
接入概览
已接入VPC
17 个
地域：北京,成都,重庆
身份接入
iOA
企业微信 56 个组织；79 个员工
微信身份 20 个
已接入域名
18 个
WEB域名：12 个
规格信息
升级扩容
查看计价
授权运维实例
10 个
剩余运维实例：4 个
可接入微信
20 个

资产接入

最近更新时间：2024-04-22 17:25:33

资产接入是指将资产所在的网络与零信任运维实例网络打通，从而实现后续的访问控制等功能。在**接入管理** > 资产接入 页面中，您可以启用运维资产所在的 VPC，接入运维资产至零信任运维实例。

以 VPC 粒度进行资产接入

选择需要接入的资产所在的 VPC，单击右侧的，接入零信任运维。开启开关后当前 VPC 下的资产可以通过零信任运维的访问网络进行运维。

说明：

- 请确认需要接入的 VPC 所在地域已启用零信任运维实例，否则将不会出现在可接入的 VPC 列表中。
- 如果需要接入的 VPC 所在地域未绑定运维公网 IP，则当前 VPC 仅限公网资产可运维，详情请参见 实例管理 。
- 开启会在被开启的 VPC 下创建一个29段子网用于引流。

身份接入

最近更新时间：2024-04-22 17:25:33

1. 登录 云防火墙控制台，在左侧导航中，选择**零信任运维 > 接入管理**。
2. 在**接入管理 > 身份管理**页面中，您可以从 iOA 中导入现有身份体系用于有端运维，也可以手动添加微信身份进行无端运维。

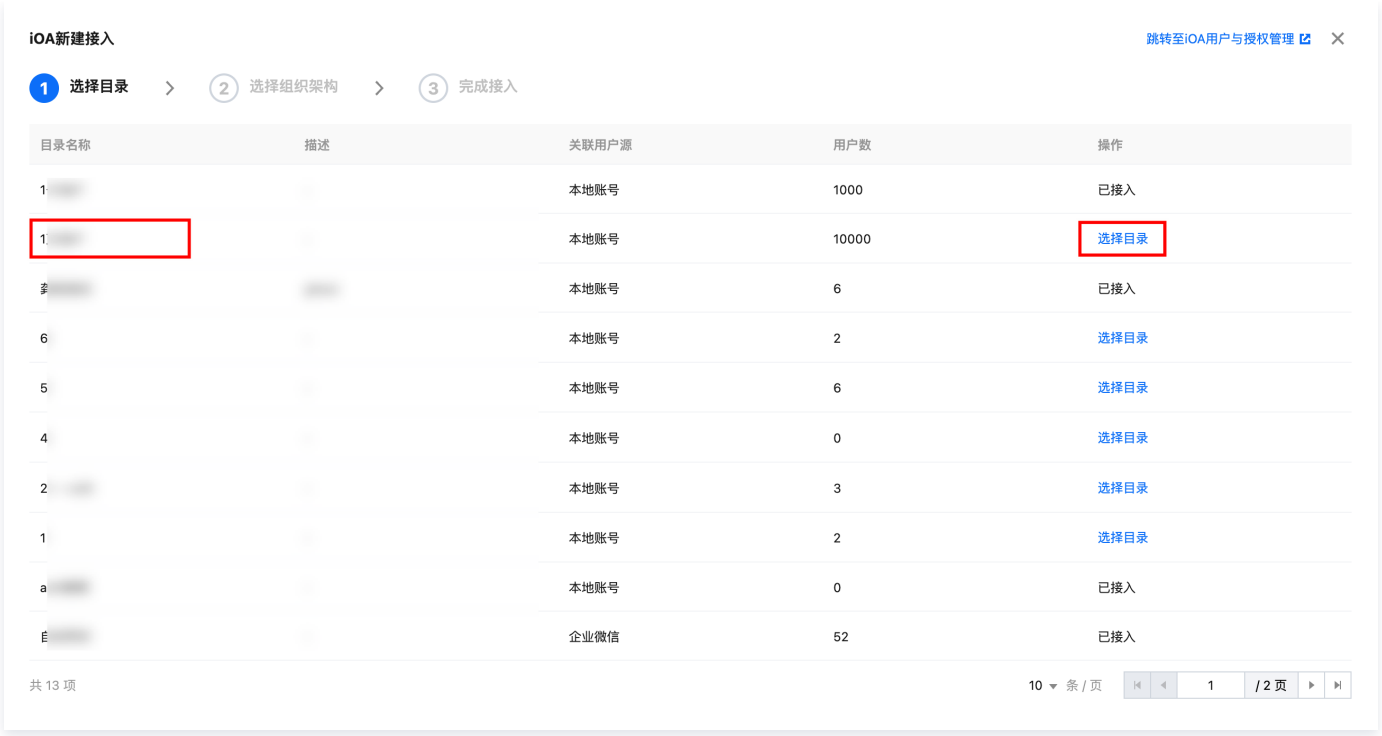
接入 iOA 身份目录

在接入 iOA 身份前，请确保您已购买 零信任运维扩展包 并完成了 iOA 零信任安全管理系统 的配置和部署。

1. 云防火墙会通过角色授权获取您的身份目录信息，需要您单击**开始授权**进行角色授权。

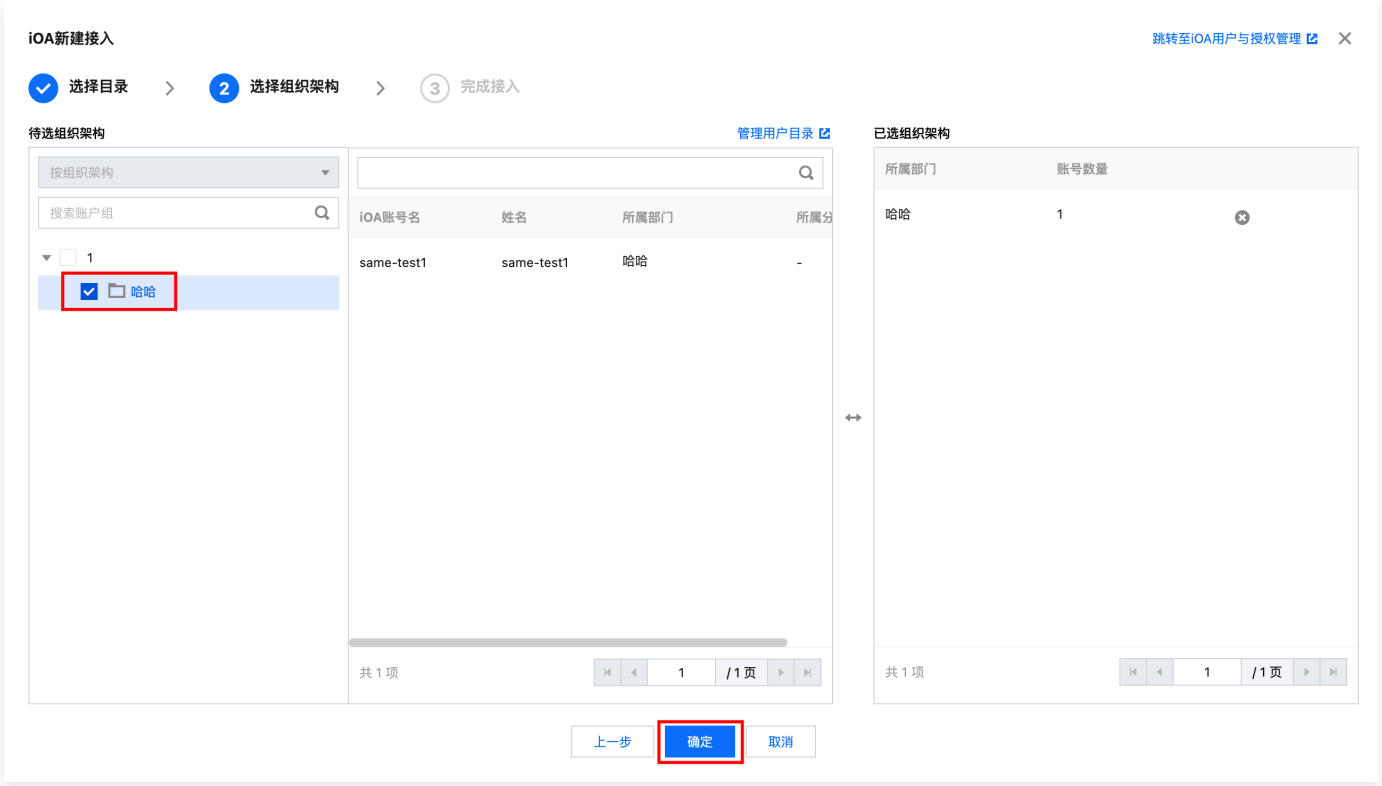
2. 单击**新增接入**，发起 iOA 目录的接入流程。

3. 选择需要接入的目录，单击右侧的**选择目录**。

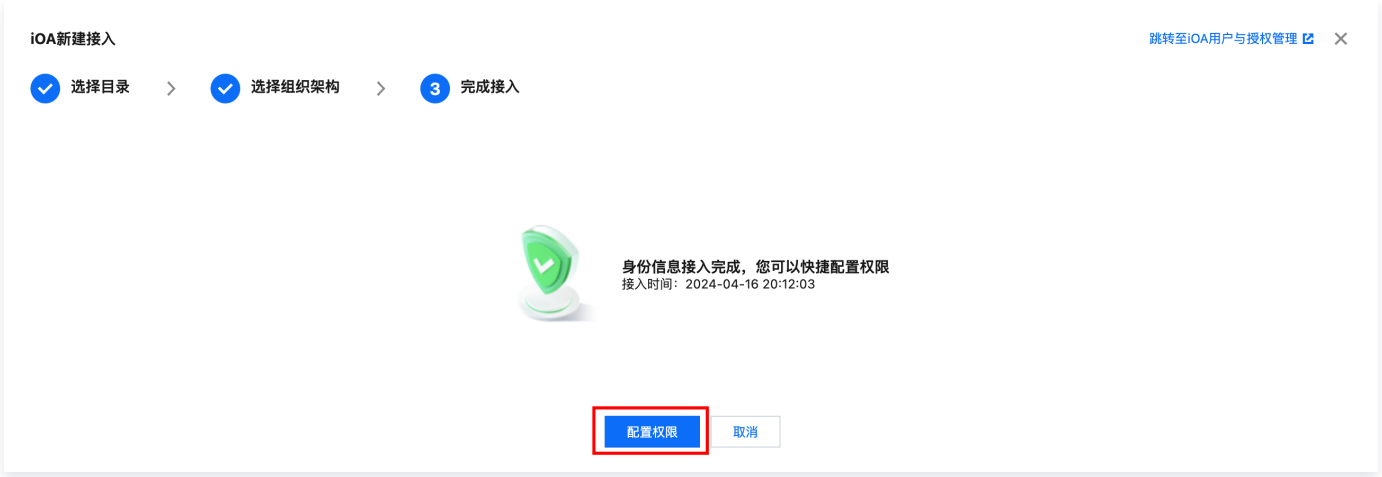


4. 选择当前目录下需要接入的组织架构，核对其包含的账号信息，确认无误后单击**确定**。

> **说明：**
> - 仅支持按组织架构导入身份信息，支持选择子目录。
> - 所选目录下新增身份或组织将会自动同步。



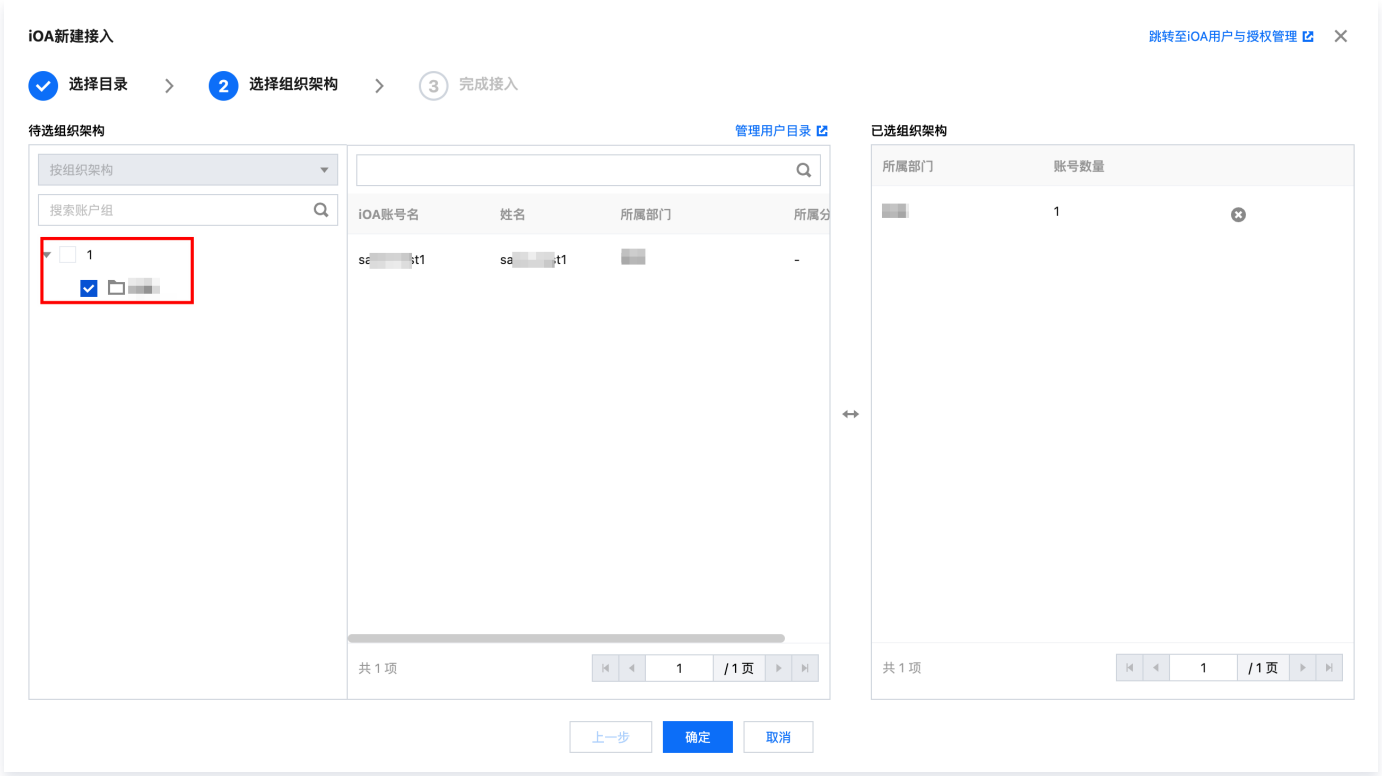
5. 完成接入，您可以通过快捷配置权限的按钮针对刚刚导入的身份信息配置运维权限，详情请参见 身份视角-新增权限 。



编辑已接入 iOA 身份目录

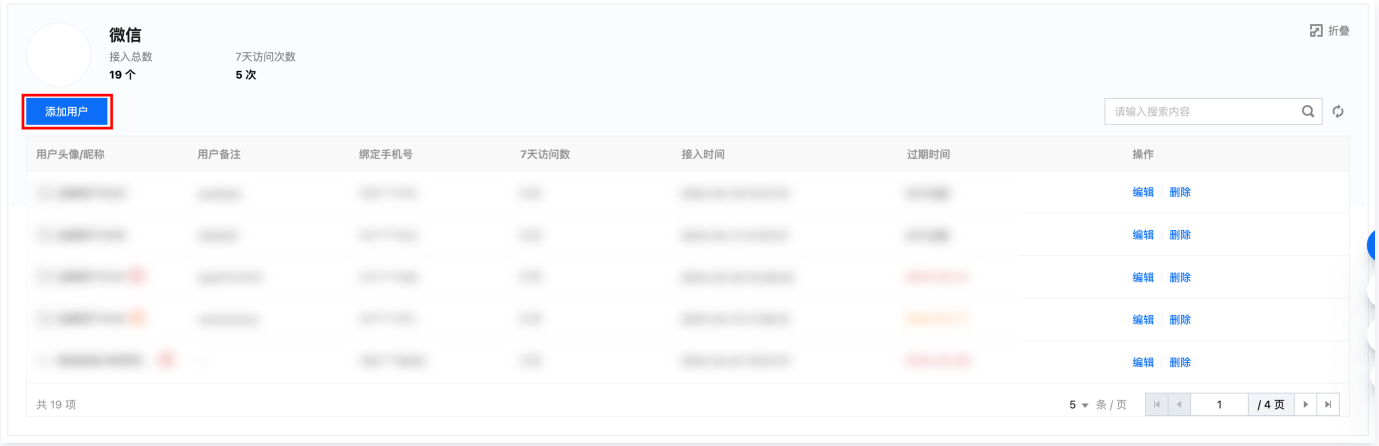
1. 选择需要编辑的目录，单击右侧的**修改配置**。

2. 您可以修改当前目录下想要接入的组织架构，单击**确定**保存。



添加微信用户

1. 在微信身份管理部分，单击**添加用户**。

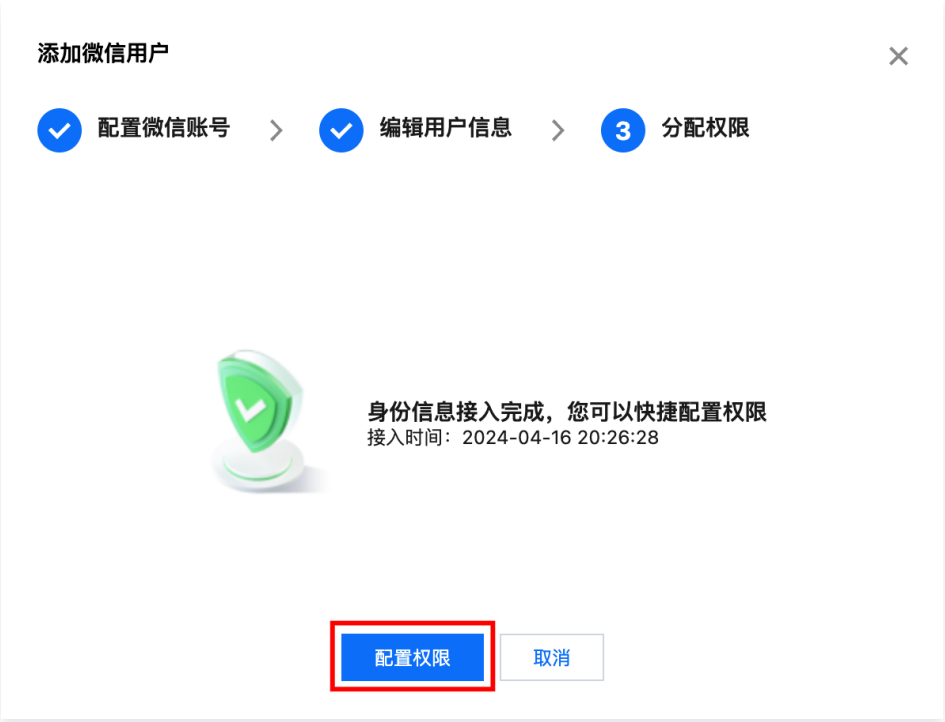


2. 在配置微信账号弹窗中，输入运维用户微信绑定的手机号，单击**下一步**。

3. 在编辑用户信息弹窗中，单击**点击获取授权**扫码获取用户微信授权，输入用户备注，设置账户过期时间，单击**提交**。

> **说明：**
> 如果无法当场获取授权，也可以跳过获取微信昵称与头像信息，提前为用户预设权限信息；等待用户进行微信扫码登录后，系统会自动获取用户的手机号及头像和昵称并匹配。

4. 提交后，完成微信用户的添加，您可以通过快捷配置权限的按钮针对刚刚添加的微信用户配置运维权限，详情请参见 身份视角-新增权限 。



编辑微信用户

1. 选择需要编辑的微信用户，单击右侧的**编辑**。

2. 您可以修改当前微信用户的备注和过期时间。

域名接入

最近更新时间：2025-04-14 16:41:31

1. 登录 云防火墙控制台，在左侧导航中，选择**零信任运维 > 接入管理**。
2. 在**接入管理 > 域名接入**页面中，您可以添加运维域名和 Web 服务域名，用于公网访问的无端运维。

接入运维域名

运维域名用于指定地域下资产 SSH、RDP、数据库的公网远程登录和运维，仅限四层协议访问，接入后可实现通过公网访问域名代理。

1. 单击**接入域名**，选择**运维域名**。

2. 您可通过**自有公网域名**绑定运维域名。

   自有域名绑定：请确保填入的域名已备案，否则可能无法正常接入。

   操作步骤：选择自有公网域名选项，选择域名需要关联的地域，并填入自有域名地址，单击确定。

3. 完成接入。

   请在接入完成后，将自有公网域名的解析地址修改至列表中提供的 cname。

接入 Web 域名

Web 域名是用于资产 Web 网站访问的域名，请确保域名已备案。接入后可实现通过公网的反向代理访问，支持公网防护及身份访问控制。

1. 单击**接入域名**，选择 **Web 域名**。

2. Web 域名支持接入自有公网域名和内网域名，请确保填入的域名已备案，否则可能无法正常接入。根据提示选择域名需要关联的地域，并填入自定义的子域名前缀。

3. 关联SSL证书。

   托管SSL证书后可用于零信任中 Web 防护的 HTTPS 访问，您需要从腾讯云托管证书中选择，如您暂未托管请前往 SSL证书控制台 管理。

> **注意：**
> 若您需要使用公网 Web 服务的无端运维，请确保关联域名已托管证书，否则将无法接入。

4. **单击确定，完成接入。**

   请在接入完成后，尽快将自有域名的解析地址修改至列表中提供的 cname。

> **注意：**
> Web 域名仅限通过公网访问。如果您之前域名已挂载Web服务，请在完成 域名绑定 后再切换解析地址，否则可能找不到真实服务地址导致访问失败。

资产管理
概述

最近更新时间：2024-04-23 15:18:21

资产管理模块主要负责使用零信任运维的运维资产配置工作，运维资产分为三类：服务器、Web 服务和数据库。在这个模块中您可以指定服务器的运维端口、托管服务器密码密钥、添加 Web 服务、绑定 Web 域名并进行公网防护和无端运维、管理数据库资产等。

- 服务器：云上的 CVM 服务器资源，支持 Windows 或 Linux。
- Web 服务：云上的 Web 服务资源，其后端地址需要在腾讯云上。
- 数据库：云上的数据库类型资产，支持类型请参见 数据库管理 。

服务器管理

最近更新时间：2025-04-27 10:13:22

1. 登录 云防火墙控制台，在左侧导航中，选择**零信任运维 > 资产管理**。
2. 在**资产管理 > 服务器**页面中，您可以对全部 CVM 服务器进行运维参数的配置，支持对接入的访问权限进行管理，方便从服务器视角查看具有权限的人员和组织。

配置运维参数

云防火墙支持对 Windows 和 Linux 类型的服务器进行远程运维，支持配置如下运维参数。

配置运维端口

云防火墙零信任远程运维支持修改非标准运维端口，从而实现公网的反向代理运维连接。

> **说明：**
> 使用公网进行无端远程运维时，请确保运维端口已配置正确，否则将无法正常连接。使用 iOA 进行内网运维不受此参数影响，请在运维时输入对应端口直接进行连接。

1. 在服务器页面，选择对应服务器，单击**协议端口**列右侧的**编辑**。

2. 在协议端口中，修改运维端口，单击**确定**。

密码密钥托管

云防火墙零信任远程运维支持托管服务器的密码密钥，从而避免密码密钥从员工泄露，实现基于身份的免密登录。

> **说明：**
> SSH 登录支持托管用户名和密码或密钥，RDP 登录仅支持托管用户名密码。

1. 在服务器页面，选择对应服务器，单击**密码密钥**列右侧的**编辑**。

> **说明：**
>
> 资产密钥类型分为未托管、已托管、密码异常三类。单击密码密钥处做相应的修改。
>
> - 未托管：实例的登录密码没有被云防火墙托管，进行远程运维的时候需要输入一遍密码。
> - 已托管：已经被云防火墙托管的实例。
> - 密码异常：密码出现异常的实例。

2. 在密码密钥窗口中，单击**添加用户名密码**填写用户名及密码，或单击**添加用户名密钥**填写用户名并上传密钥。

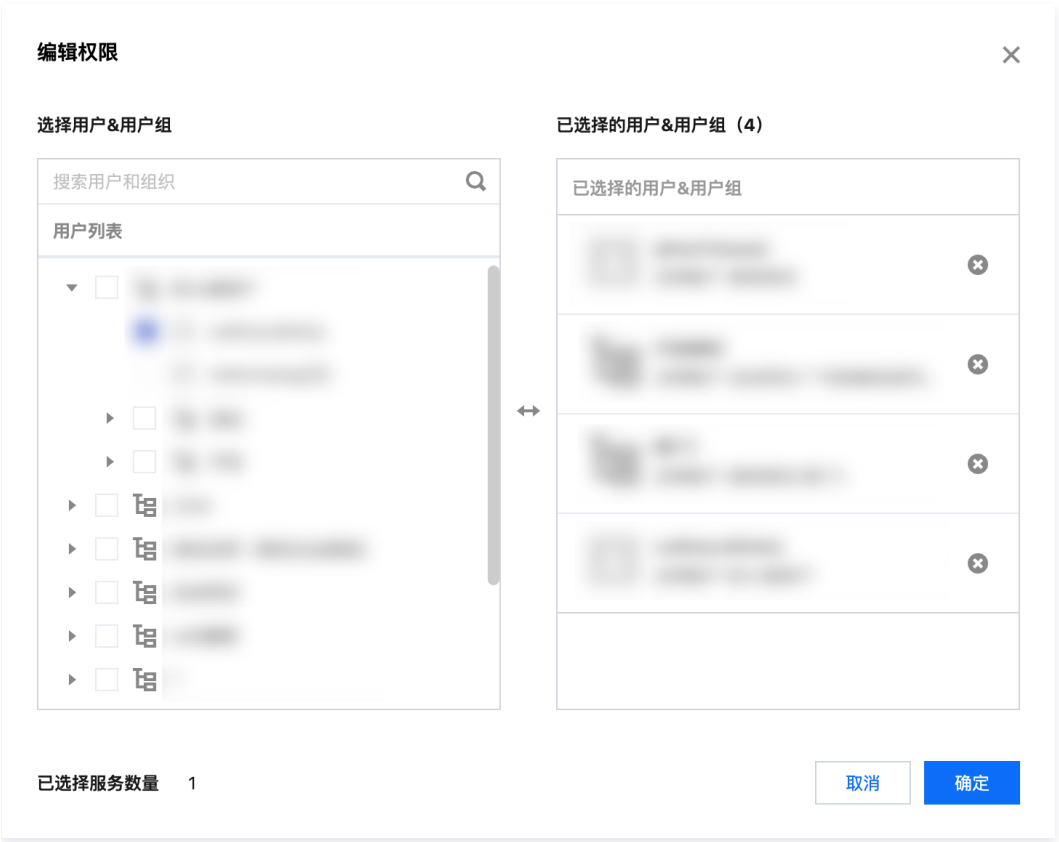
3. 单击**确定**，完成编辑。

管理权限

1. 在服务器页面，可查看全部服务器类型资产列表及所授权用户。
2. 单击**管理权限**，可对实例所授权的运维用户进行管理，支持解绑用户与新增用户。

3. 在编辑权限弹窗中可以新增或删除权限，勾选左侧用户和组织即为新增权限，单击右侧 即为删除权限。

> **说明：**
> 编辑权限页面仅可编辑身份视角下添加的规则权限，如果需要编辑继承下来的权限请前往 权限管理 的规则视角对规则进行编辑。



4. 单击**确定**，保存配置。

查看登录日志

零信任运维日志记录了服务器资产实例的运维记录，便于后续审计。

在 服务器页面，单击**登录日志**，可跳转至**零信任运维日志 > 服务器登录**页面，展示当前服务器实例的人员登录日志。支持登录回放的功能，便于追溯用户的操作行为。

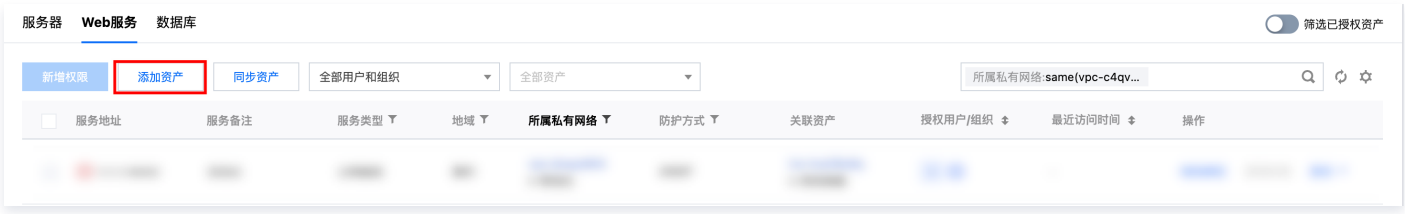
Web 服务管理

最近更新时间：2024-04-22 17:25:33

1. 登录 云防火墙控制台，在左侧导航中，选择**零信任运维 > 资产管理**。
2. 在**资产管理 > Web 服务**页面中，您可以添加 Web 服务并配置服务地址，支持绑定域名接入公网反代实现高级防护，支持配置内网有端访问权限及公网无端访问权限，提供从 Web 服务的视角查看具有权限的人员和组织。

添加 Web 服务

1. 在 Web 服务页面，单击**添加资产**，添加您需要接入的 Web 资产地址。



2. 在添加资产弹窗中，配置 Web 服务的信息，单击**确定**。
   - 关联实例：Web 服务部署位置所在的服务器，用于接入零信任运维网络。
   - 服务地址：Web 服务绑定的 IP 地址及端口，支持通过公网连接或内网连接。
   - 服务备注：用来管理 Web 服务资产的备注信息，方便后续统一维护和展示。

> **注意：**
> 请确认 Web 服务关联的服务器资产所在 VPC 已开启资产接入开关，否则可能无法关联至对应资产。

删除 Web 服务

1. 在 Web 服务页面，单击**更多 > 删除服务**。

2. 在确认删除窗口中，单击**确定**，即可删除当前 Web 服务。

> **注意：**
> 删除将会自动取消接入防护，关联权限将会删除，请谨慎操作。

绑定域名

绑定域名可以将 Web 服务接入零信任运维实例，通过公网反代的形式隐匿真实服务地址，过滤不同身份的访问，从而避免业务暴露互联网被 Web 攻击。是一种轻量化的无端的 Web 运维方案。

使用场景

- 应用对象：需要暴露公网访问地址的 Web 服务，可能是公网服务或内网服务。
- 应用场景：需要对 Web 服务进行身份访问限制，拦截 Web 攻击。希望隐匿真实服务地址通过域名访问。

操作步骤

1. 完成 添加资产 后，在 Web 服务页面，单击 Web 服务右侧的**域名绑定**。

2. 在域名绑定弹窗中，选择**一个已接入的 Web 域名**。

> **注意：**
> 如果您还未完成域名接入，则无法选择对应域名。请参考 域名接入 。

3. 选择域名后，您可以选择是否启用 HTTPS 访问及配置默认的访问端口。

> **说明：**
> - 如果您在域名接入时未托管证书则不支持 HTTPS 访问。
> - 如果您需要通过公网运维并配置基于身份的访问控制规则，请选择启用 HTTPS。

4. 选择公网防护方案。
   - **基础防护：提供基于前端对抗和前端挑战的基础防护，对人机、攻击者等进行有效过滤，可直接通过域名访问，不支持公网的访问控制。**
   - **高级防护：包含基础防护功能，访问服务前需通过微信或 iOA 进行身份认证，高级防护仅支持 HTTPS 协议。**

> **说明：**
> **公网防护仅限公网通过绑定的域名访问 Web 服务，iOA 有端访问请使用真实服务地址直接连接。**

5. 单击**下一步**，对当前 Web 服务进行权限配置。
   - 如果防护方式选择**基础防护**，则**权限控制仅会生效于 iOA 的有端访问**，公网访问不受限制。
   - 如果防护方式选择**高级防护**，则需要选择绑定的用户，单击**确定**即可生成配置。

> **说明：**
> 极简模式下访问所选服务不再限制用户，身份认证通过后即可进行实名制访问。该模式下会记录所有访问用户的用户信息。

6. 单击**确定**，即可完成域名绑定及权限配置操作。

> **说明：**
> 完成域名绑定后，您仍可通过真实服务地址进行访问，这种访问会绕过防火墙的权限管控，建议使用防火墙封禁真实服务访问地址。

取消域名绑定

1. 在 Web 服务页面，选择需要取消绑定的 Web 服务，单击右侧的**修改绑定**。

2. 在修改绑定窗口中，单击**取消绑定**，即可完成解绑操作。

管理权限

1. 在 Web 服务页面，可查看已添加的 Web 服务资产列表及所授权用户。
2. 单击**管理权限**，可对 Web 服务所授权的运维用户进行管理，支持解绑用户与新增用户。

3. 在编辑权限弹窗中可以新增或删除权限，勾选左侧用户和组织即为新增权限，单击右侧即为删除权限。

> **说明：**
> 编辑权限页面仅可编辑身份视角下添加的规则权限，如果需要编辑继承下来的权限请前往 权限管理 的规则视角对规则进行编辑。

编辑权限
极简模式：访问不限用户，仅需使用微信或iOA认证后即可访问
选择用户&用户组
已选择的用户&用户组（5）
搜索用户和组织
用户列表
已选择的用户&用户组
已选择服务数量 1
取消
确定

4. 单击**确定**，保存配置。

数据库管理

最近更新时间：2024-04-22 17:25:33

1. 登录 **云防火墙控制台**，在左侧导航中，选择**零信任运维 > 资产管理**。
2. 在**资产管理 > 数据库页**面中，您可以添对数据库资产进行统一查看，对接入的访问权限进行概览，方便从数据库视角查看具有权限的人员和组织。

> **说明：**
> 当前版本仅支持 MySQL、MariaDB、Redis、CKafka、ElasticSearch 五种数据库类型，暂不支持通过数据库视角编辑权限。

查看授权用户/组织

您可以在列表中将鼠标悬浮在**授权用户/组织**列，查看已授权的用户或组织。

查看访问日志

您可以在列表右侧操作区单击**访问日志**，跳转至零信任运维日志中查看当前数据库的所有访问记录。

权限管理
概述

最近更新时间：2024-04-22 17:25:33

权限管理模块主要负责对接入的身份信息和资产信息进行权限下发和管控。整体上，它可以分为身份视角和规则视角两部分。

- 身份视角：即从人或组织的视角查看其拥有资产的权限信息。
- 规则视角：即从白名单规则的视角管理访问控制权限。

身份视角下权限配置更直观，更精准；规则视角倾向于大规模或批量下发权限，更适合人员或资产较多、变化较快的用户。

版权所有：腾讯云计算（北京）有限责任公司

身份视角

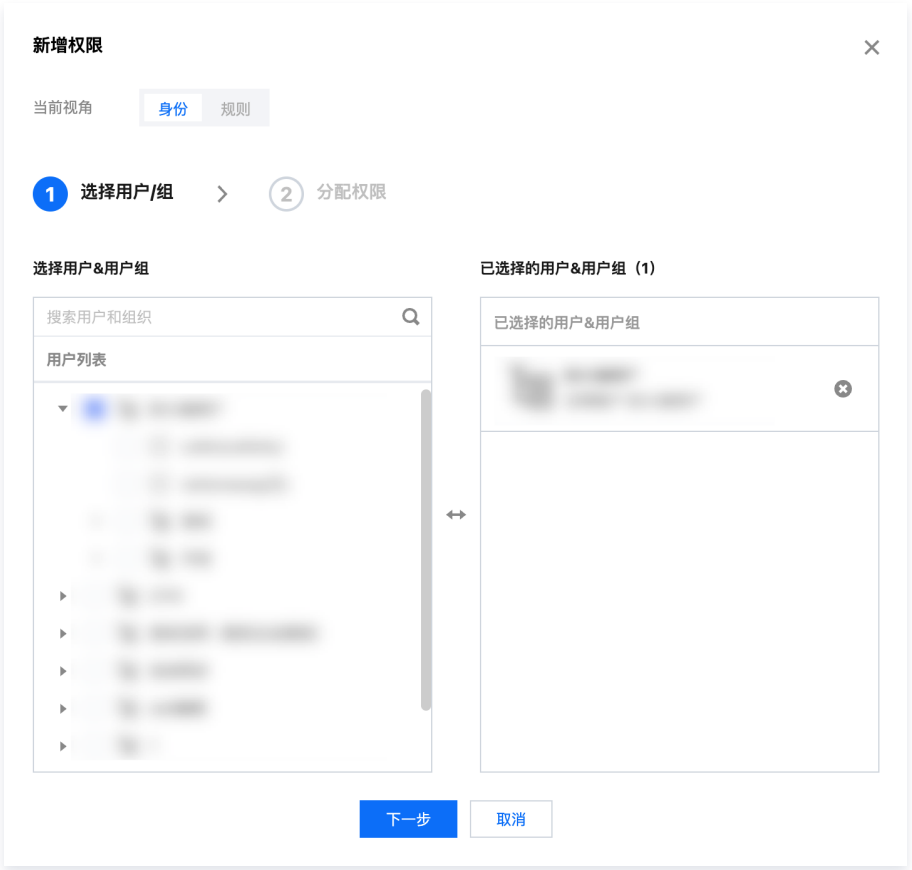
最近更新时间：2024-04-22 17:25:33

身份视角即从人或组织的视角查看其拥有资产的权限信息。

新增权限

1. 登录 云防火墙控制台，在左侧导航中，选择**零信任运维 > 权限管理**。
2. 在权限管理，单击**新增权限**。

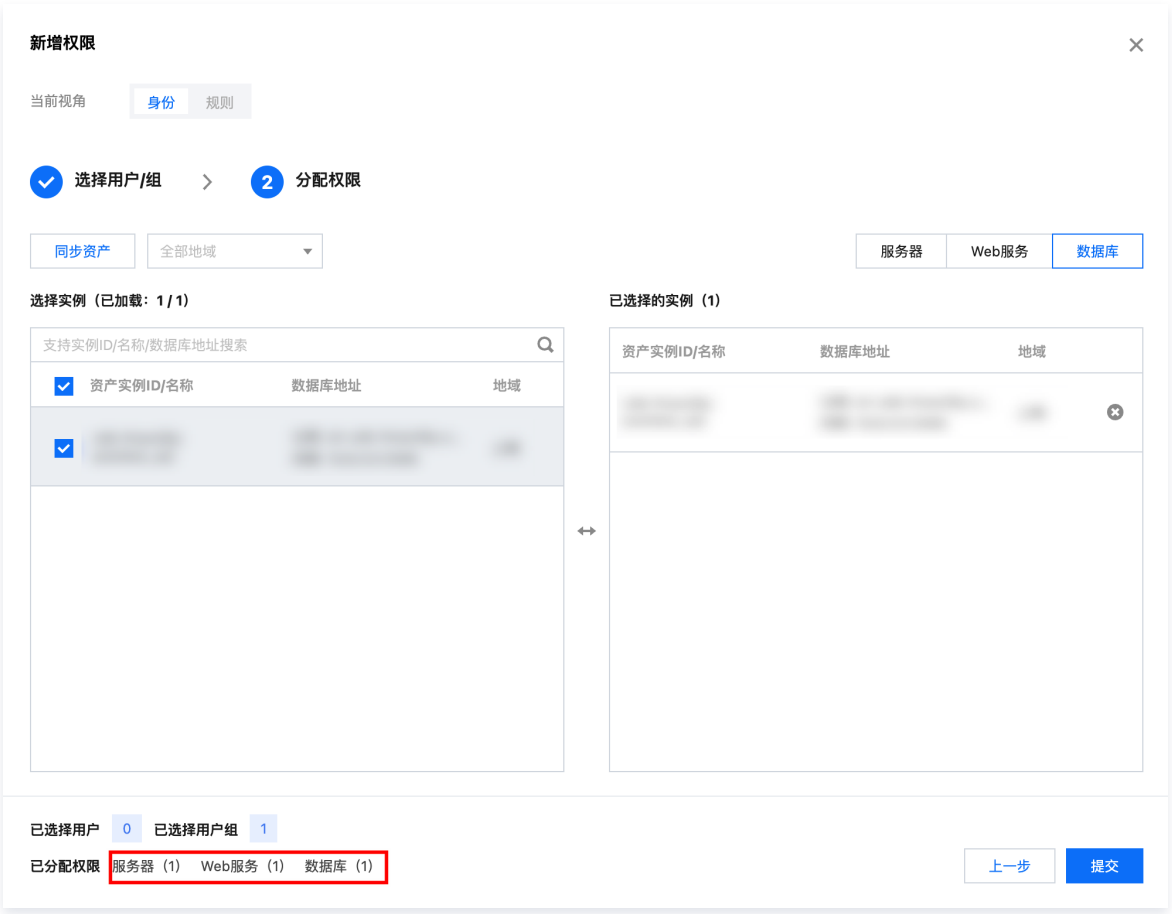
3. 选择身份视角，选择用户/用户组，勾选后，在已选择的用户/用户组确认所选的授权用户，单击**下一步**。



> **说明：**
> 当选择了用户组时，是对该组织架构赋予权限，即使后续组织用户成员发生变化，其组织下的所有用户均有访问权限。

4. 对选中的用户/用户组，分配资产权限，包括服务器资产、Web 服务资产、数据库资产。

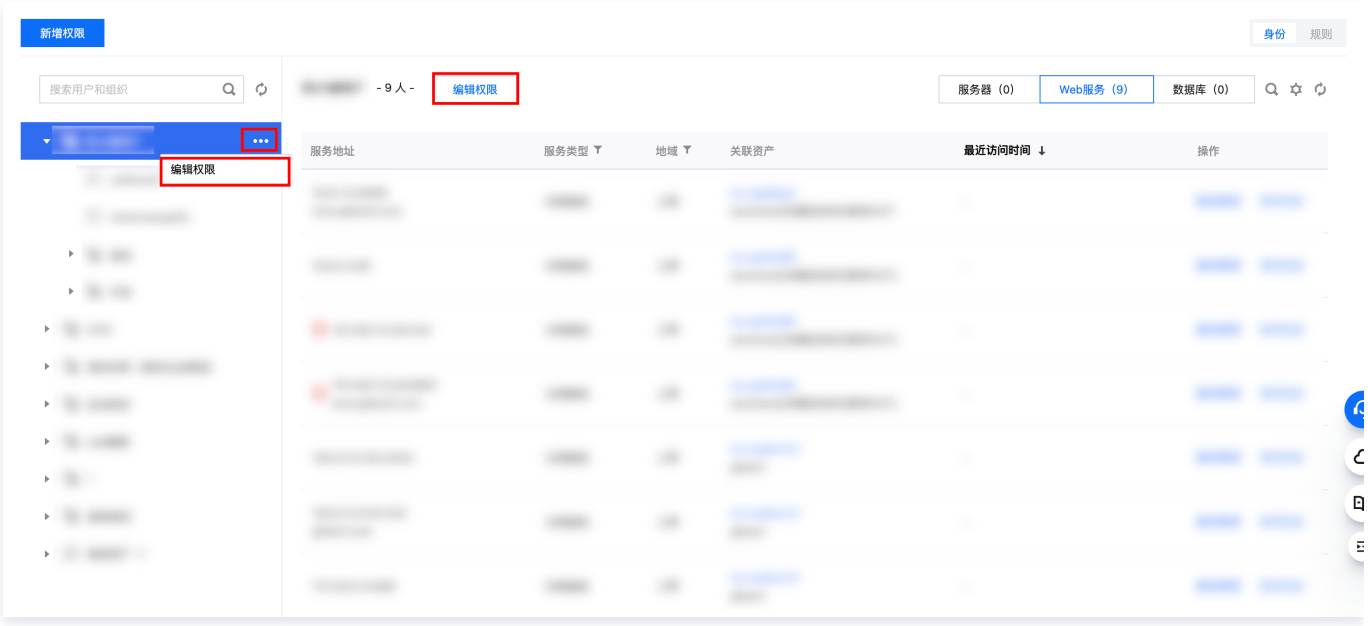
   支持按照地域与资产类型筛选资产进行选择，勾选分配资产后，弹窗下方会显示当前已选择的用户与用户组数量，以及分配的运维实例与 Web 服务数量，确认无误后，单击**提交**完成新增权限。



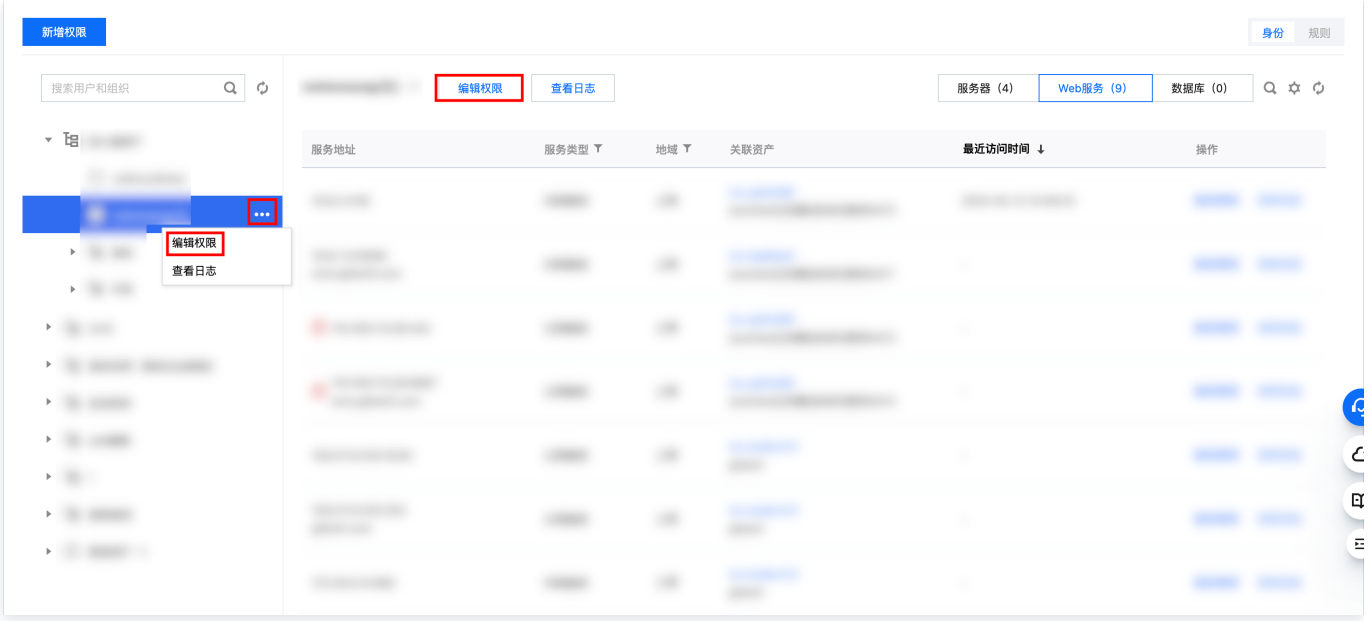
编辑权限

支持对单个用户或用户组织进行编辑权限。

1. 在 权限管理页面，选择身份视角，选中需要编辑权限的用户/用户组，在页面右侧出现该用户/用户组权限对应的可访问资产。
2. 单击头像右侧的 ···，出现用户身份操作选项。单击**编辑权限**，均支持编辑用户/用户组身份权限。
   - 组织



   - 用户

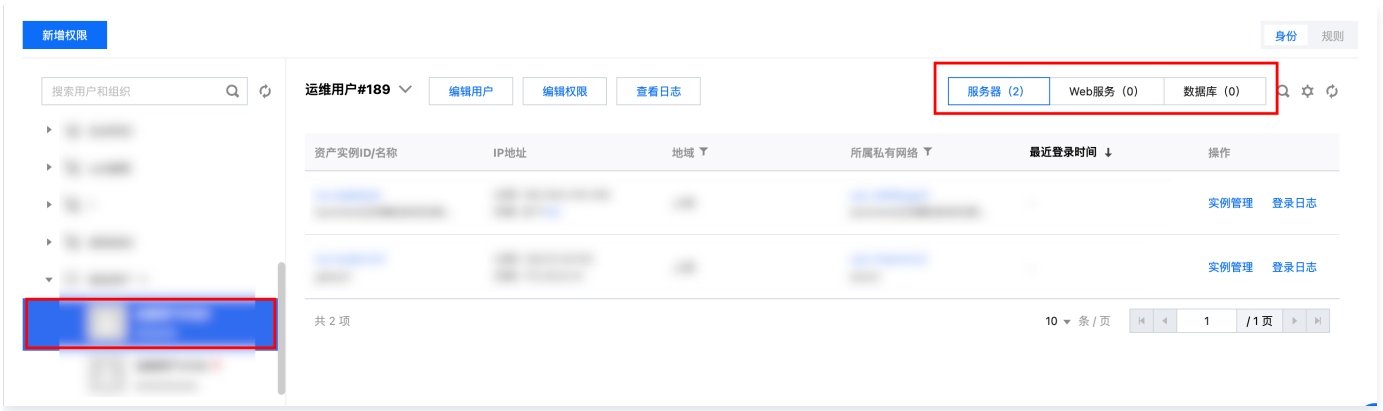


3. 在编辑用户权限弹窗中，重新选择授权该用户/用户组访问的资产，弹窗下方会显示该用户/用户组当前已分配的资产权限数量，确认无误后，单击**确定**完成权限编辑。

> **注意：**
> 编辑权限页面仅可编辑身份视角下添加的规则权限，如果需要编辑继承下来的权限请前往 **权限管理** 的规则视角对规则进行编辑。

查看权限

在 **权限管理页面**，选中需要查看权限的用户/用户组，在页面右侧出现该用户/用户组权限对应的可访问资产，包括服务器、Web 服务、数据库类型，支持查看资产实例名称/ID、IP 地址、地域、所属私有网络、最近登录时间等信息。


新增权限
身份
规则
搜索用户和组织
运维用户#189
编辑用户
编辑权限
查看日志
服务器（2）
Web服务（0）
数据库（0）
资产实例ID/名称
IP地址
地域
所属私有网络
最近登录时间
操作
实例管理
登录日志
实例管理
登录日志
共 2 项
10 条 / 页
1
/ 1 页

规则视角

最近更新时间：2024-04-22 17:25:33

规则视角即从白名单规则的视角管理访问控制权限。

新增权限

1. 登录 云防火墙控制台，在左侧导航中，选择**零信任运维 > 权限管理**。
2. 在权限管理，单击**新增权限**。

3. 选择规则视角，填写访问源、访问目的及描述。

参数名称	说明
访问源类型	• 个人：选中后可选择 iOA 中的个人用户或微信用户。 • 组织：可选择 iOA 中的组织或全部微信用户。
访问目的类型	• 服务器：选择服务器类型资产。 • Web 服务：选择 Web 服务类型资产。 **注意：** 当身份信息选择了 iOA 身份后，不限制 Web 服务类型；若身份信息选择微信身份，则 Web 服务仅可选择已绑定域名且防护类型为高级防护的资产。 • 数据库：选择数据库类型资产。 **注意：**

> 不支持微信身份，仅限 iOA 内网有端运维。

- 资产分组：选择资产分组，云防火墙会自动下发权限至资产分组下的服务器类型和数据库类型资产。
- 标签：选择资源标签，云防火墙会自动下发权限至资源标签关联的服务器类型和数据库类型资产。

4. 单击**确定**，云防火墙会自动根据填写的身份信息和授权资产下发访问权限，您也可以在身份视角或对应资产处查看到对应权限。权限下发可能会有延迟，请耐心等待。

编辑权限

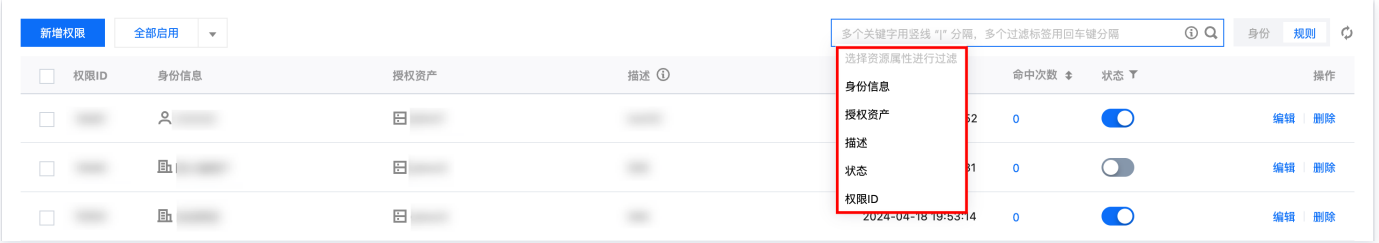
1. 找到想要修改的权限，单击右侧的**编辑**。

2. 您可以在权限编辑态中修改身份信息、授权资产或描述。具体字段请参考新增权限。

查看权限

1. 登录 云防火墙控制台，在左侧导航中，选择**零信任运维 > 权限管理**。
2. 在权限管理，单击规则切换至规则视角。

3. 您可以在下方的权限列表中查看所有具备权限的规则内容。
4. 支持按照权限 ID、身份信息、授权资产、描述进行权限检索。



登录方式
微信用户公网远程登录服务器

最近更新时间：2024-05-06 17:03:51

接入零信任运维的用户登录权限配置后，使用域名进行远程登录验证配置是否生效。

快速入门

本视频为您介绍如何快速上手微信远程运维。
观看视频

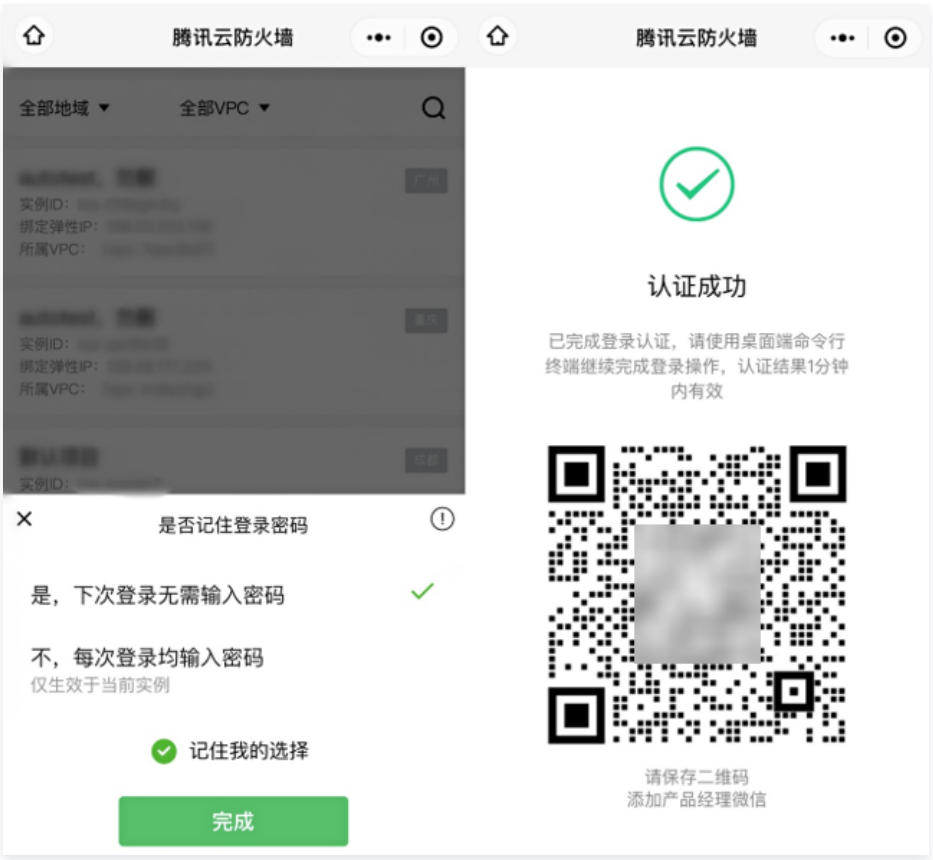
类型为 SSH 的登录方法

1. 命令行输入命令：
   - 方式1：使用用户名登录，输入命令 ssh 用户名`@cfw.tencentcs.com`，例如 `ssh abc123@cfw.tencentcs.com`。
   - 方式2：使用 root 用户登录，输入命令 `ssh root@cfw.tencentcs.com`。
2. 云防火墙会在命令行返回一个二维码，使用之前在控制台的接入微信身份权限中绑定的微信扫描此二维码。

> **说明：**
> 如果二维码没有正常展示，在末尾处会有一个 URL 网址，访问此网址也可以展示二维码。

3. 在微信中，选择腾讯云账号和实例，进行授权登录。

4. 授权登录后，请在1分钟内完成登录操作，否则需要重新授权。如果选择记住登录密码，云防火墙会记录用户在命令行登录的密码，后续登录不再需要手动登录，即使变更密码，防火墙也会自动记录新密码。

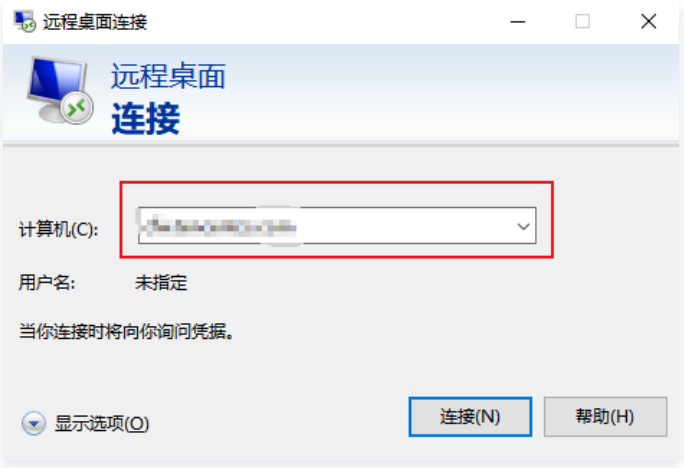


说明：

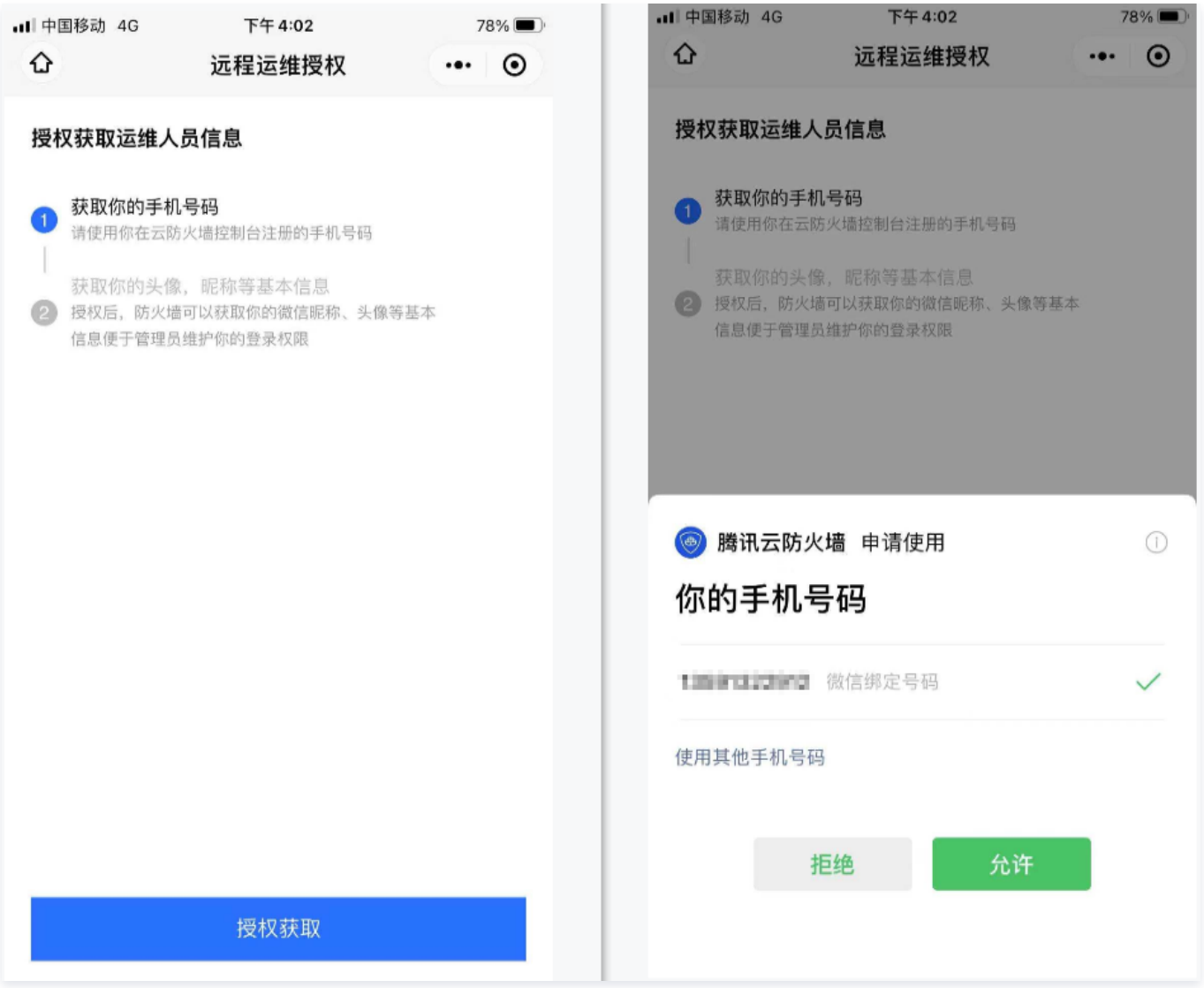
- 若操作系统为 Windows，则类型为 RDP，端口为3389。
- 若操作系统为其他，则类型为 SSH，端口为22。
- 若扫描的 SSH 的二维码，则仅展示 SSH 的实例列表。
- 若扫描 RDP 的二维码，则仅展示 RDP 的实例列表。

类型为 RDP 的登录方法

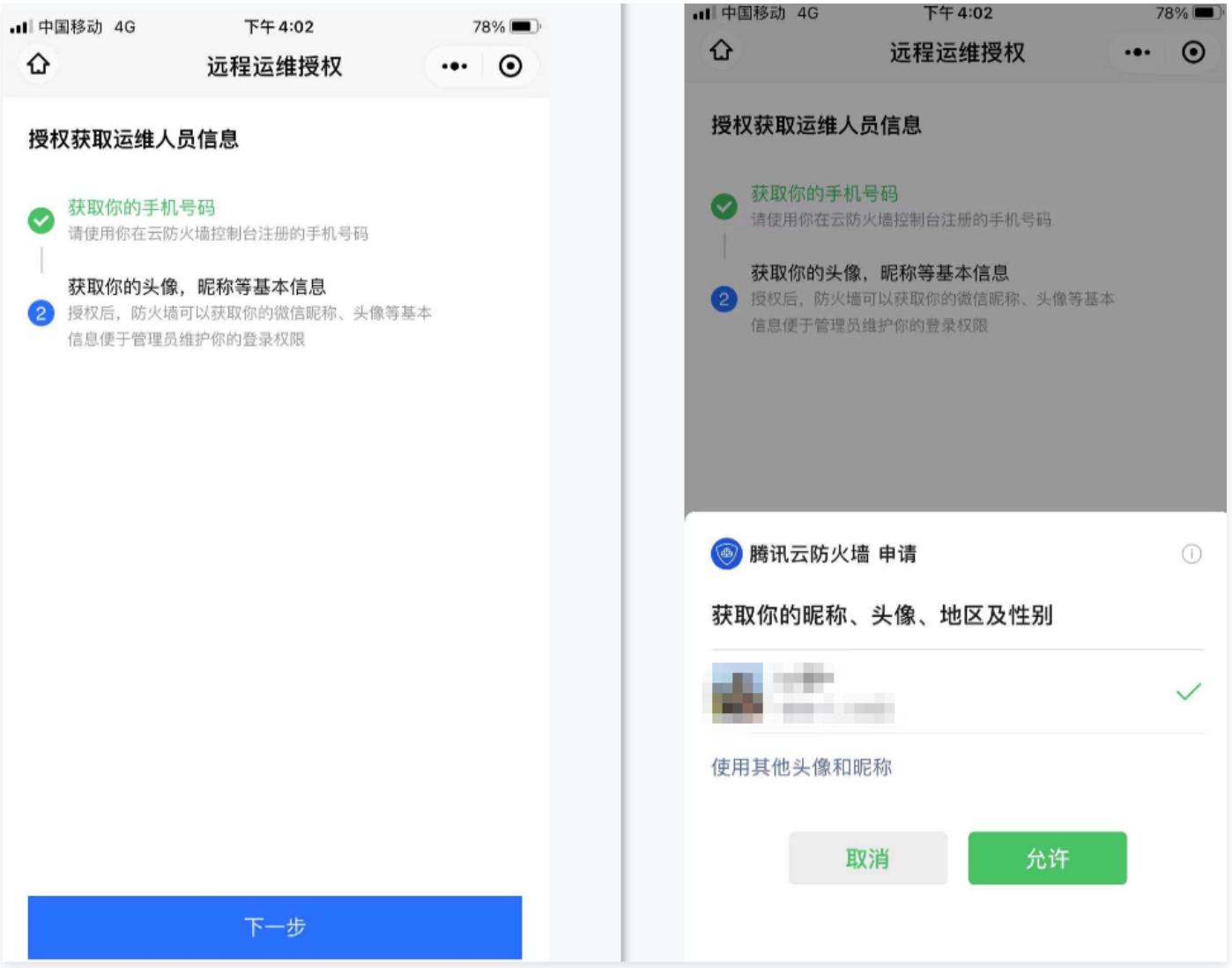
1. 运维人员在机器上，打开远程运维桌面功能，输入控制台指定的域名，单击**连接**，返回二维码的页面。



2. 运维人员扫授权二维码，获取手机号。



3. 获取微信头像和昵称，单击**允许**后授权成功。



4. 选择需要登录的实例，验证完成即可远程运维，授权登录后，请在1分钟内完成登录操作，否则需要重新授权。

说明：

- 若操作系统为 Windows，则类型为 RDP，端口为3389。
- 若操作系统为其他，则类型为 SSH，端口为22。
- 若扫描的 SSH 的二维码，则仅展示 SSH 的实例列表。
- 若扫描 RDP 的二维码，则仅展示 RDP 的实例列表。

iOA 用户内网访问运维资产

最近更新时间：2024-04-23 15:33:42

前提条件

1. 已完成 iOA 身份目录接入 。
2. 已 配置用户权限 。
3. 已登录 iOA 终端设备。
4. 通过 iOA 代理的内网访问运维资产。

访问方式

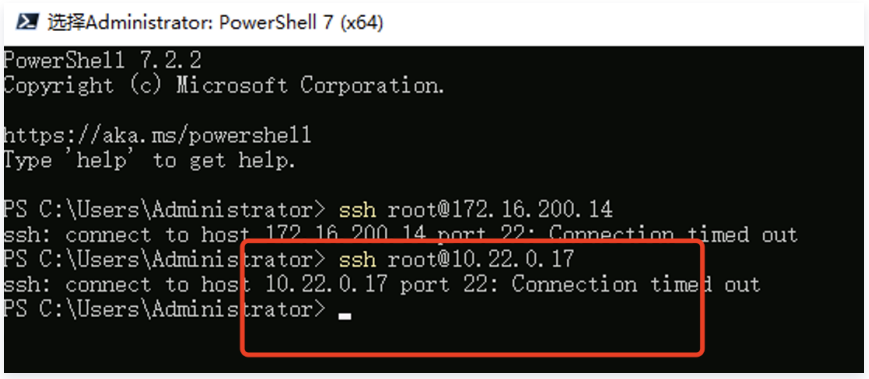
iOA 用户支持直接通过内网访问服务器类型、Web 服务类型、数据库类型的运维资产。

> **说明：**
> 请直接通过资产的真实地址进行访问，若通过绑定的域名访问将不会使用内网直连运维资产。

服务器资产登录

1. 命令行直接输入用户名密码及服务器地址进行连接。例如：`ssh root@192.168.0.9 -p 2222` 。
2. 如果您拥有对应服务器的权限，可直接继续下一步操作。

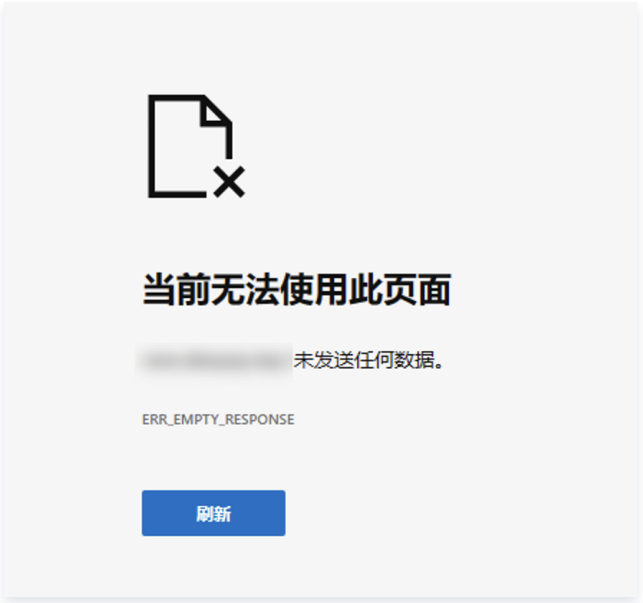
3. 如果您没有权限，可能会提示连接超时。



Web 服务资产访问

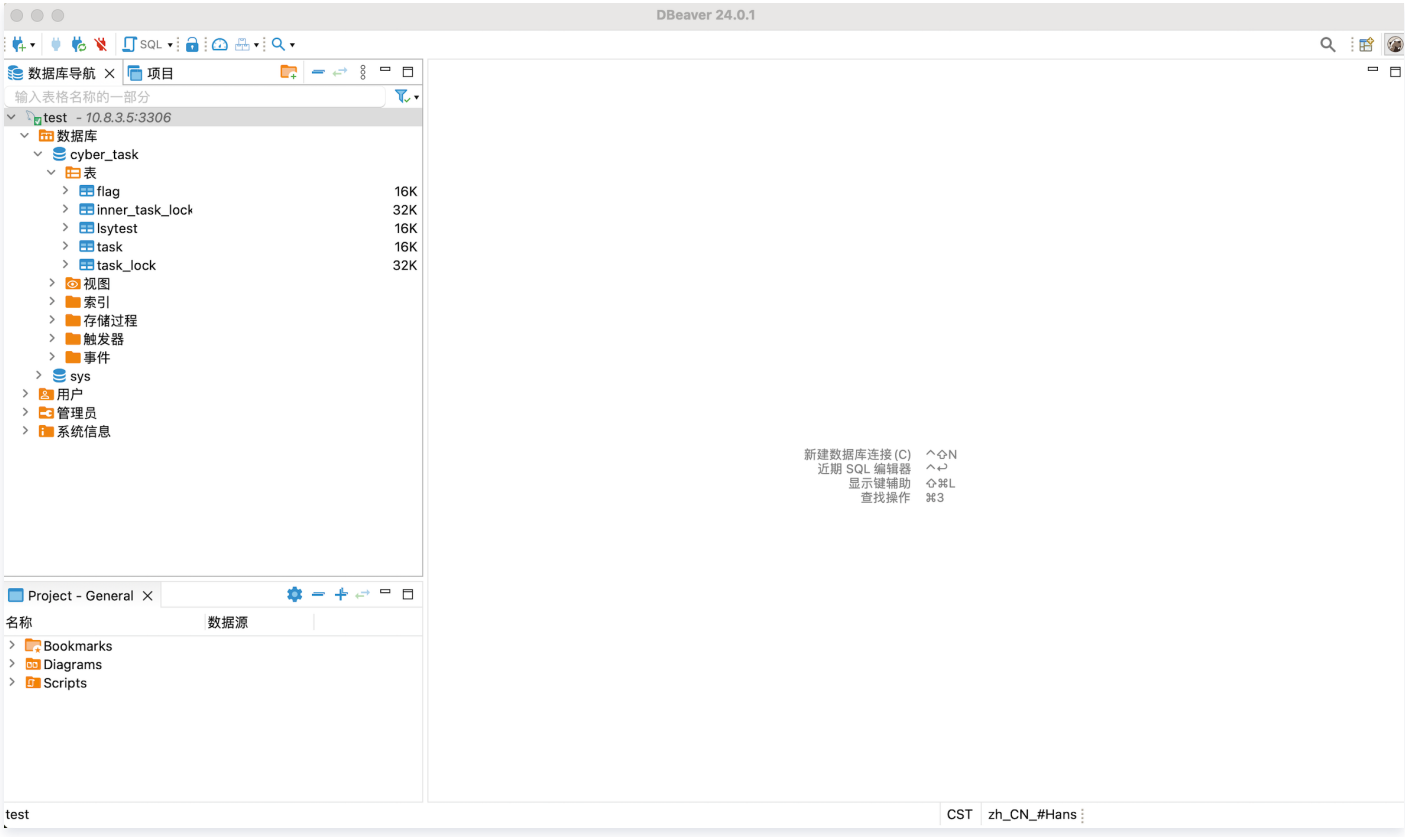
1. 浏览器直接输入真实的服务地址进行连接，例如：`https://192.168.0.9/` 。
2. 如果您拥有对应服务器的权限，可直接继续下一步操作。

3. 如果您没有权限，可能会提示无响应。



数据库资产登录

1. 您可以通过数据库自有协议或命令行与对应数据库进行连接。
2. 如果您拥有对应数据库的权限，可直接继续下一步操作，否则会连接超时无法访问。



3. 如果您没有权限，可能会提示连接超时。

微信或 iOA 用户公网访问 Web 服务

最近更新时间：2024-04-23 15:33:42

访问前置条件

1. 已完成 域名绑定 。
2. 已修改域名解析地址。
3. 已 配置用户权限 。
4. 通过公网访问 Web 服务。

访问方式

1. 在浏览器直接输入绑定的域名进行访问，会弹出身份校验的二维码。
2. 请使用具有权限的微信账号扫描二维码进行身份确认。

3. 如果是 iOA 用户您也可以点单击下方的**其他登录方式**，跳转至 iOA 进行身份验证。

4. 认证通过后即可访问 Web 服务。

网络蜜罐

概述

最近更新时间：2023-02-16 11:22:26

网络蜜罐是一种在互联网上运行的仿真业务系统，实际不会承载任何的真实业务。网络蜜罐通过探针暴露在用户的网络中，例如被攻击者踩中，则会主动记录攻击者信息并追溯攻击手法，为真实业务的防御提供准确的攻击者情报与反制溯源能力。同时，网络蜜罐在重保场景中，为真实业务争取足够的时间，达到防守成功的目的。
腾讯云防火墙的蜜罐服务部署在腾讯云蜜场中，不占用用户的网络空间，并且通过部署不同的 VPC 实现相互隔离，即使攻击者进入，也不会造成横向移动的情况。蜜罐的暴露探针部署在用户的网络中，可以是 IP 或域名，并通过将指定端口/路径的流量转发到不同的蜜罐服务，实现在业务系统中部署“陷阱”。

使用网络蜜罐

1. 新建探针，并开启。
2. 管理探针。
3. 新建蜜罐服务，绑定探针。
4. 管理蜜罐服务。
5. 防御溯源，查看网络蜜罐告警与日志。

主要功能

基于腾讯云防火墙的蜜罐服务，有如下三个主要功能：

- 仿真程度高，不易被攻击者识破。
- 可收集攻击者信息，提供给防守方的反制能力。
- 可拖延攻击者时间，为网络安全保护提供时间保障。

业务系统的安全性与探针数量成正比，且不会过多占用用户的网络资源，通过蜜场中的高真实度的仿真服务，达到“欺骗”攻击者的目的。

告警与日志

攻击欺骗事件告警

在**告警中心** > 攻击欺骗事件 页面，可查看网络蜜罐探测到的攻击欺骗事件详情。

网络蜜罐欺骗日志

在**日志审计** > **入侵防御日志** > 网络蜜罐 页面，可查看网络蜜罐探测到的攻击欺骗事件的日志信息。
网络蜜罐操作日志
在**日志审计** > **操作日志** > 网络蜜罐操作 页面，可查看网络蜜罐功能的操作详情和对应账号。

版本支持说明

云防火墙高级版、企业版和旗舰版均支持购买蜜罐服务配额，详情请参见 购买指南 。

版权所有：腾讯云计算（北京）有限责任公司

新建探针

最近更新时间：2025-04-14 16:41:31

暴露探针是在用户业务系统中部署的“陷阱”，可以是 IP 或域名，能将指定端口/路径的流量转发到指定的蜜罐服务中，从而记录攻击者信息并追溯攻击手法，因此网络蜜罐服务需要和暴露探针关联后才能正常运行。
用户在进入网络蜜罐控制台时会默认进入**探针暴露**页面。建议用户先新建探针，而后新建蜜罐并与相应探针关联。

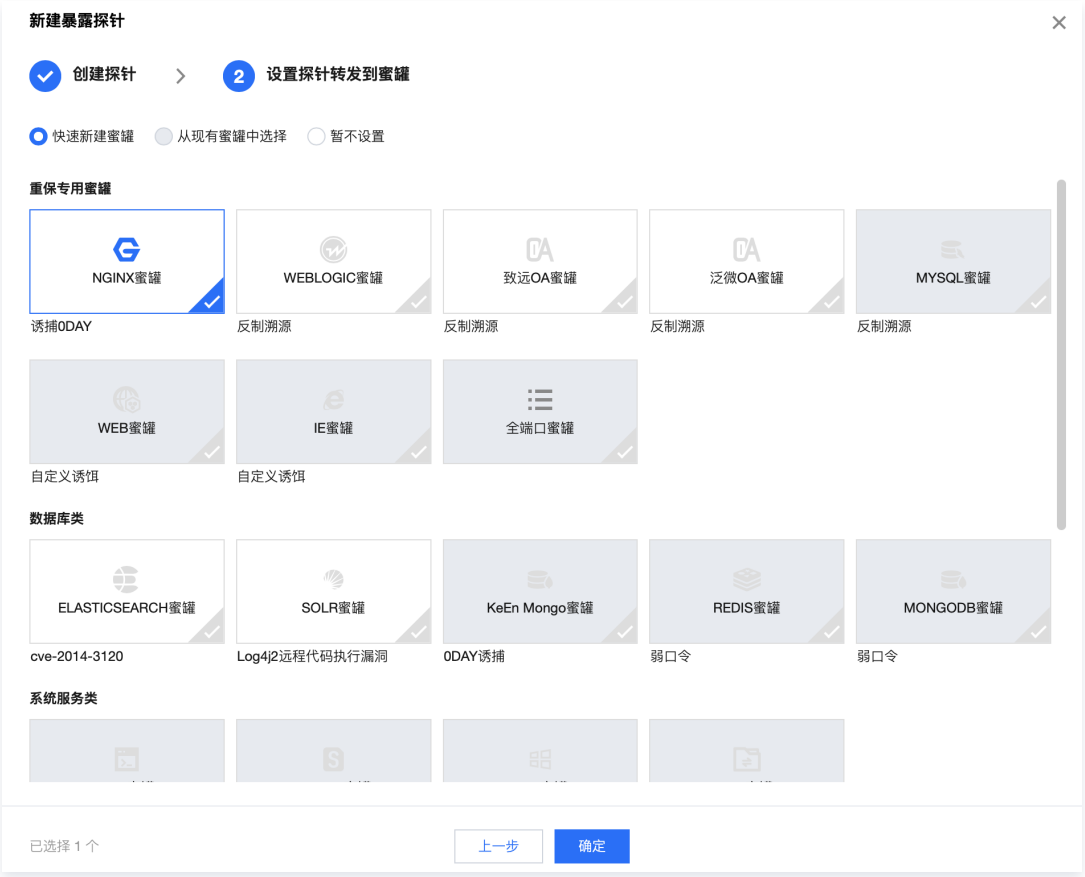
1. 登录 云防火墙控制台，在左侧导航栏中，单击**网络蜜罐** > **探针暴露**。
2. 在探针暴露页面，单击**新建探针**。

3. 在新建探针暴露弹窗中，选择地域，实例名称、部署模式以及弹性 IP，单击**下一步**。

参数	说明

地域	支持国内部分地域（具体地域可登录 云防火墙控制台 > **网络蜜罐** > **新建探针** > **地域**查看），创建实例后不可更改。
实例名称	自定义实例名。
部署模式	• 内网 IP　选择一个子网，我们会自动新建一个弹性网卡与内网 IP，这个 IP 的指定端口可以设置转发到蜜罐服务中。 • 公网 IP　选择现有的一个公网 IP 部署探针，该 IP上的指定端口的流量将会转发到蜜罐服务中。 • 负载均衡：选择现有的一个负载均衡实例部署探针，指定域名上的路径的流量将会转发到蜜罐服务中。
选择子网	当部署模式为内网 IP 时，需配置该内容。
IP 地址	当部署模式为内网 IP 时，需配置该内容。
弹性 IP	当部署模式为公网 IP 时，需配置该内容。选择新建弹性 IP。
部署实例	当部署模式为负载均衡时，需配置该内容。根据实际需求配置。
域名	当部署模式为负载均衡时，需配置该内容。根据实际需求配置。
转发器	当部署模式为负载均衡时，需配置该内容。请在当前负载均衡实例所属的私有网络中选择一个云服务器实例作为当前监听器的后端服务，仅支持 Linux 系统的云服务器。
转发蜜罐服务	支持快速新建蜜罐、从现有蜜罐中选择或暂不设置。

4. **设置转发蜜罐服务，单击确定，即可完成新建。**



- 快速新建蜜罐：单击**快速新建蜜罐**，勾选所需蜜罐服务即可，可多选。

  > **说明：**
  > 由于 WEB 蜜罐需要将现有的 SSH/MySQL 蜜罐作为诱饵，因此 WEB 蜜罐在快速选择后不会自动关联诱饵。当用户在新建探针时单击快速选择蜜罐并选择 WEB 蜜罐时，蜜罐服务并未开始工作。用户需要到蜜罐服务中找到相应的 WEB 蜜罐编辑并关联相应的 SSH/MySQL 蜜罐后，该蜜罐服务开始工作。

- 从现有蜜罐中选择：单击**从现有蜜罐中选择**，选择所需蜜罐服务，可多选，并根据需求可修改监听端口或输入路径。

> **说明：**
> - 当部署模式为公网 IP 时，可修改监听端口。
> - 当部署模式为负载均衡时，部分蜜罐可支持自定义路径，详情以控制台为准。

5. 支持单个或批量开启探针。
   - 单个：选择目标探针，单击开关列的，在“确认开启”弹窗中，单击**确定**，即可开启单个探针。

   - 批量：选中一个或多个探针，单击**开启探针**，在“确认开启”弹窗中，单击**确定**，开启多个探针。

管理探针

最近更新时间：2024-05-17 16:06:51

对已建立的暴露探针，进行编辑、删除、筛选、排序等操作。

编辑配置

1. 登录 云防火墙控制台，在左侧导航栏中，单击**网络蜜罐 > 探针暴露页面**。
2. 在探针暴露页面，选择目标探针，单击操作列的**编辑**。

3. 在编辑探针暴露弹窗中，可修改实例名称和转发到蜜罐服务的探针端口/路径，单击**确定**，即可保存修改。

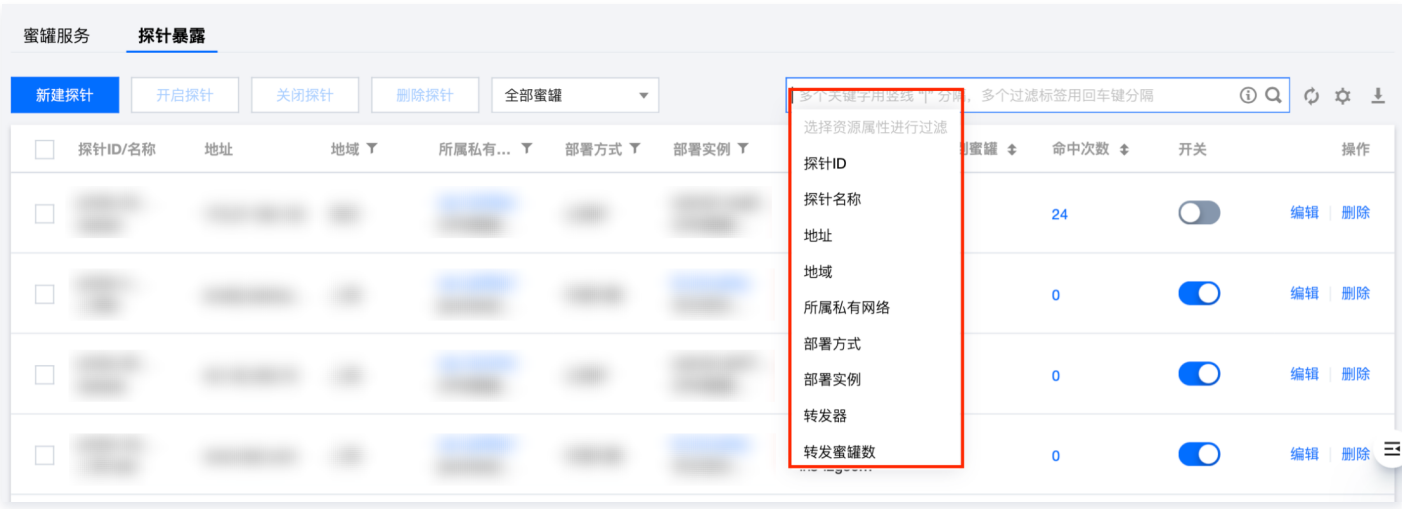
删除探针

1. 在 探针暴露页面，支持单个或批量删除探针。
   - 单个：选择目标探针，单击操作列的**删除**，在“确认删除”弹窗中，单击**确定**，即可删除单个探针。

- 批量：选中一个或多个探针，单击**删除**，在“确认删除”弹窗中，单击**确定**，即可删除选中探针。

筛选/排序

- 在 探针暴露页面，单击搜索框，支持通过“探针 ID、探针名称”等关键词对探针暴露事件进行筛选。



- 单击图中探针暴露列表的表头“地域”、“所属私有网络”、“部署方式”、“部署实例”和“转发器”，即可对探针暴露事件进行筛选。

- 单击图中探针暴露列表的表头“转发到蜜罐”和 “命中次数”，可以按照升序或降序显示探针暴露事件。

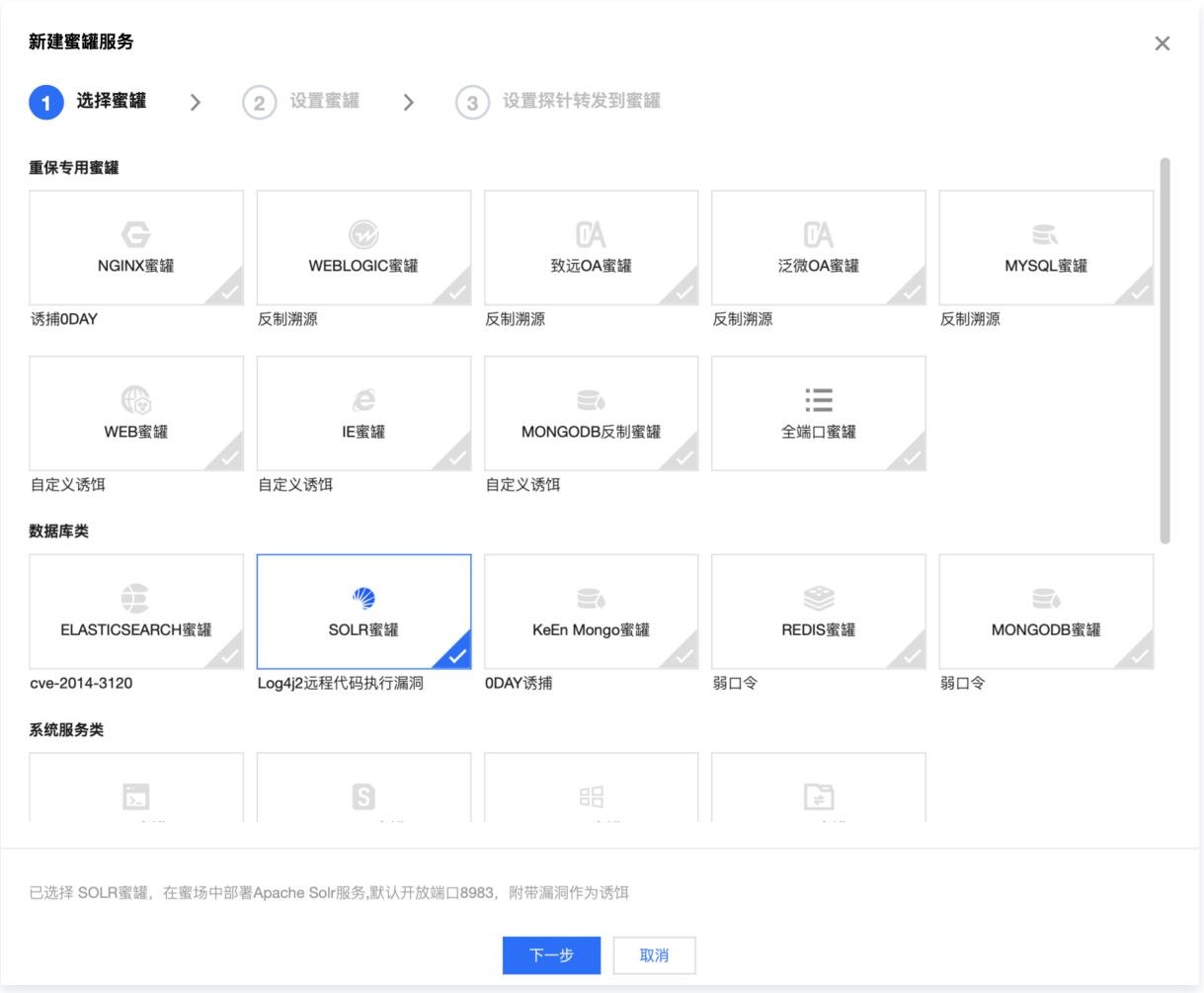
新建蜜罐服务

最近更新时间：2024-05-17 16:06:51

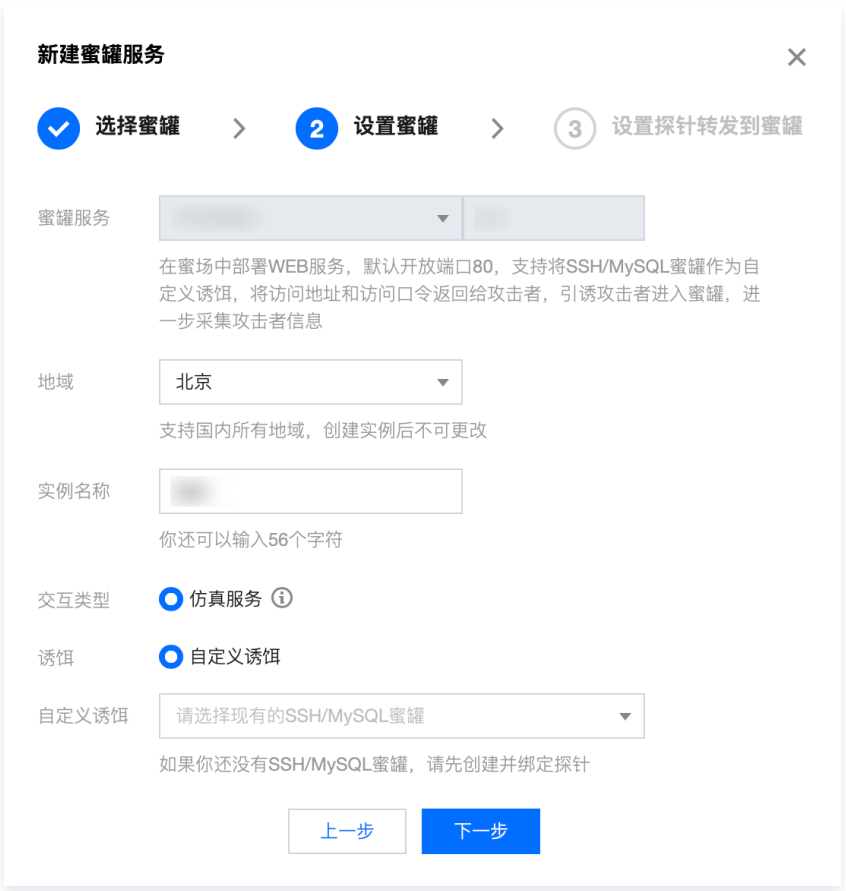
网络蜜罐服务和暴露探针关联后才能正常运行，当新建完暴露探针后，需要建立与之关联的蜜罐服务。

1. 登录 云防火墙控制台，在左侧导航栏中，单击**网络蜜罐 > 蜜罐服务**。
2. 在蜜罐服务页面，单击**新建蜜罐**。

3. 在新建蜜罐服务窗口中，选定需要的蜜罐服务类型，单击**下一步**。



4. 设置蜜罐相关参数后，单击**下一步**，设置探针转发到蜜罐。



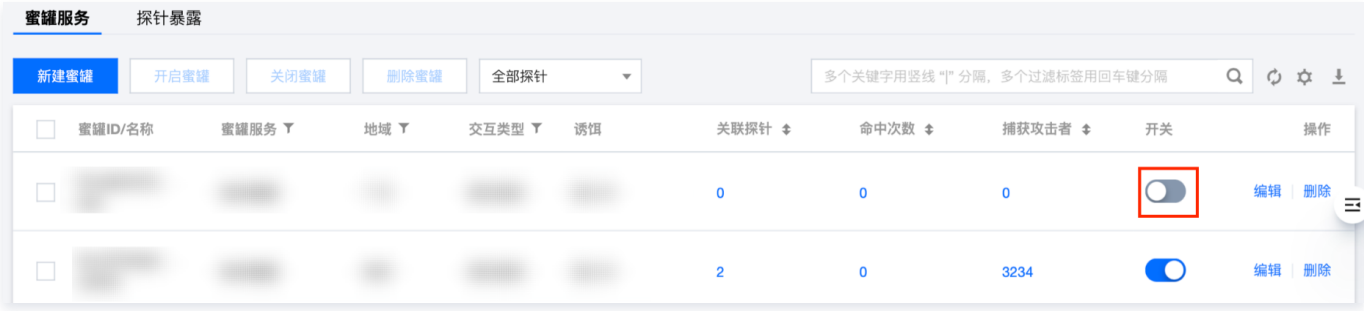
参数	说明
地域	支持国内所有地域，创建实例后不可更改。
实例名称	自定义实例名。
蜜罐服务	包括 ELASTICSEARCH 蜜罐、MYSQL 蜜罐、NGINX 蜜罐、SALTSTACK 蜜罐、SSH 蜜罐、STRUTS 蜜罐、WEBLOGIC 蜜罐和 WEB 蜜罐。其中，除 WEB 蜜罐外，其余所有类型的蜜罐均内置诱饵与脆弱性。
交互类型	• 真实服务　高交互类型，后端运行真实服务与诱饵，针对攻击者的每次请求均会真实响应，以此达到充分欺骗攻击者的目的，进而为真实防护争取时间。 • 仿真服务　中交互类型，后端运行仿真的服务与诱饵，能够根据攻击者的部分请求模拟生成对应的响应信息并诱导攻击者继续执行，从而为真实防护争取时间。
诱饵	• ELASTICSEARCH 蜜罐：cve-2014-3120。 • SALTSTACK 蜜罐：cve-2020-11651。 • SSH 蜜罐：弱口令。 • STRUTS 蜜罐：cve-2017-12611。 • WEBLOGIC 蜜罐：cve-2017-10271。 • 其他蜜罐：无。
自定义诱饵	• MYSQL 蜜罐、SSH 蜜罐：可选择登录口令，并设置密码。 • WEB 蜜罐：可选择现有的 SSH/MySQL 蜜罐作为自定义诱饵，如果还没有 SSH/MySQL 蜜罐，请先创建并绑定探针。 • 其他蜜罐：无。
设置探针	• 从现有探针中选择　选中从现有探针中选择，选择所需探针实例和端口号即可。 • 暂不设置：不绑定探针。

5. 绑定暴露探针。
   - 现有探针中选择：选中从现有探针中选择，选择所需探针实例和端口号，单击**确定**。

- 没有探针或暂不设置：暂不绑定探针，单击**确定**。

> **注意：**
> 蜜罐服务必须需要绑定探针才会生效。若选择了暂不设置，用户可以在创建蜜罐完成后，通过编辑蜜罐重新绑定探针或在探针界面与蜜罐完成绑定。

6. 支持单个或批量开启蜜罐。
   - 单个：选择目标蜜罐，单击开关列的，在“确认开启”弹窗中，单击**确定**，即可开启当前蜜罐服务。



   - 批量：选中一个或多个蜜罐，单击**开启蜜罐**，在“确认开启”弹窗中，单击**确定**，开启选中蜜罐服务。

管理蜜罐

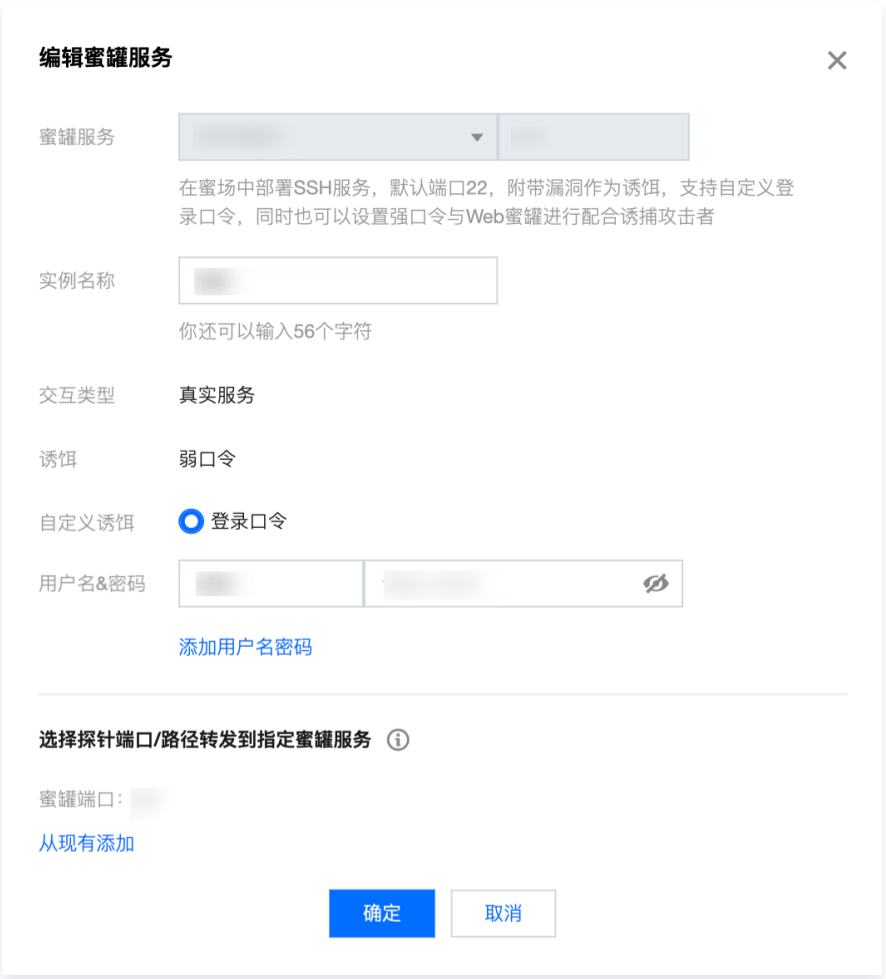
最近更新时间：2024-04-22 17:25:32

对建立好的蜜罐服务，进行编辑、删除、筛选、排序等操作。

编辑配置

1. 登录 云防火墙控制台，在左侧导航栏中，单击**网络蜜罐 > 蜜罐服务**。
2. 在蜜罐服务页面，选中蜜罐服务，单击操作列的**编辑**。

3. 在编辑蜜罐服务弹窗中，可修改实例名称和关联暴露探针，单击**确定**，即可保存修改。



删除蜜罐

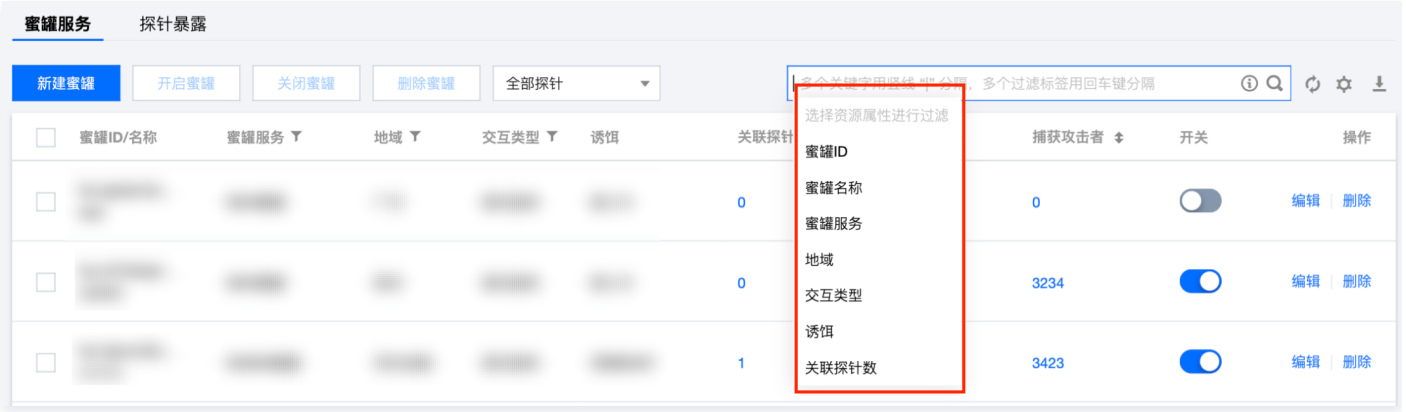
1. 在 蜜罐服务页面，支持单个或批量删除蜜罐。

- 单个：选择目标蜜罐，单击操作列的**删除**，在“确认删除”弹窗中，单击**确定**，即可删除单个蜜罐。

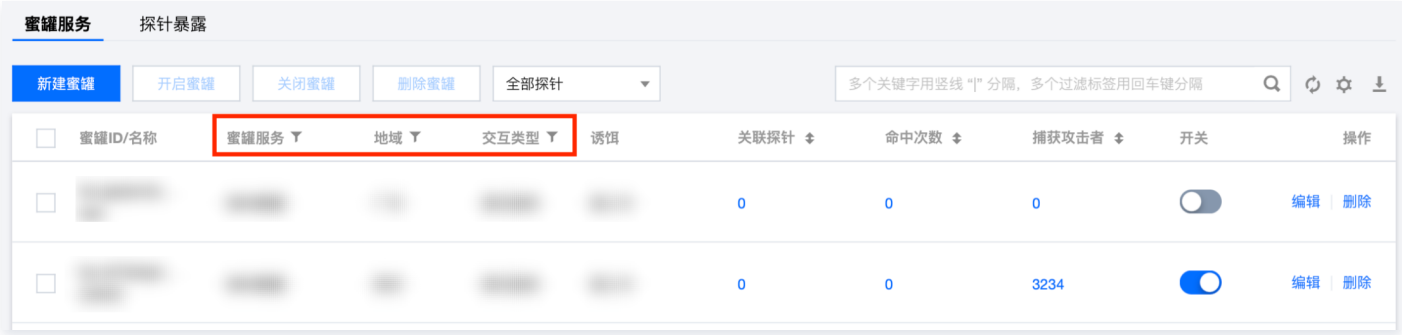
- 批量：选中一个或多个蜜罐，单击**删除**，在“确认删除”弹窗中，单击**确定**，即可删除选中蜜罐。

筛选/排序

- 在 蜜罐服务页面，单击搜索框，通过“蜜罐 ID、蜜罐名称”等关键词对蜜罐服务事件进行筛选。



- 单击蜜罐服务列表的表头“蜜罐服务”、“地域”和“交互类型”，即可对蜜罐服务事件进行筛选。



- 单击蜜罐服务列表的表头“关联探针”和 “命中次数”，可以按照升序或降序显示蜜罐服务事件。

防御溯源

最近更新时间：2024-05-17 15:57:11

查看告警

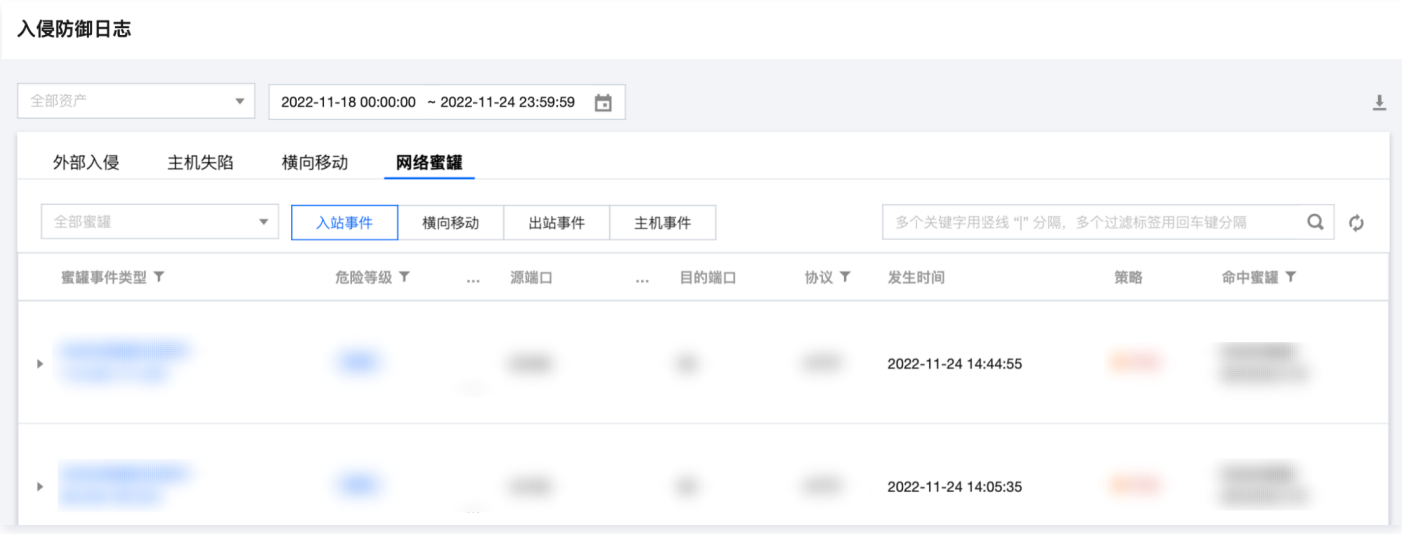
1. 登录 云防火墙控制台，在左侧导航栏中，单击**网络蜜罐 > 蜜罐服务**。
2. 在蜜罐服务页面，单击查看告警，跳转至**告警中心 > 攻击欺骗事件**，可查看网络蜜罐探测到的攻击欺骗事件详情。

> **说明：**
> 支持对产生网络蜜罐告警的危险 IP 进行封禁、放通、忽略等操作，可参见 欺骗事件查看与处理 。

查看日志

1. 在 蜜罐服务页面，单击**查看日志**，跳转至**日志审计 > 入侵防御日志 > 网络蜜罐** 。

2. 在网络蜜罐页签，可查看网络蜜罐探测到的攻击欺骗事件的日志信息。



防御概况

1. 在 蜜罐服务页面，支持快速检查蜜罐服务、探针暴露、已命中蜜罐、被扫描探针、攻击 IP 和扫描 IP 的数量。
2. 网络蜜罐配额可以根据实际情况去扩容，单击**购买配额**，进行配额购买。

蜜罐策略可视化

蜜罐策略图包括策略列表和策略视图，分别用表格和连线图的方式，展示了不同探针地址对应的不同路径，不同蜜罐服务类型和不同的诱饵类型。

策略列表

策略列表以表格的形式，详细的展示了不同探针地址对应的相应蜜罐信息。

策略视图

- 策略视图运用了连线图，直观且清晰的展示了不同地域的不同探针地址对应的蜜罐信息。

- 略视图支持通过蜜罐筛选条件寻找对应的探针地址。例如，用户可以将鼠标单击①**探针地址**和②**蜜罐服务**，来找到对应的探针和蜜罐服务对应的诱饵。若将鼠标悬浮到具体的策略连线上时，还可以显示该探针部署的地域、端口/路径、对应的蜜罐服务以及诱饵信息。

日志审计

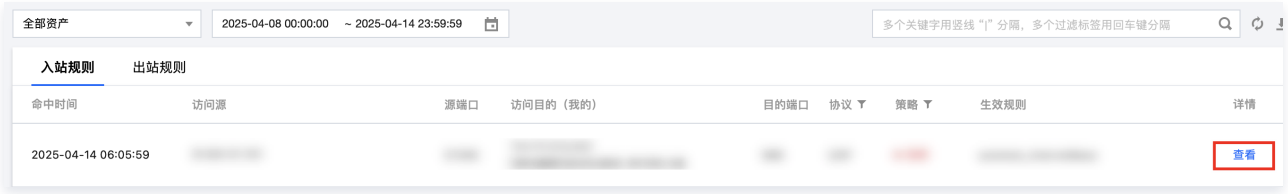
最近更新时间：2025-06-30 10:49:21

本文档将指导您查看云防火墙相关日志。

查看访问控制日志

1. 登录 云防火墙控制台，在左侧导航栏中，选择**日志审计 > 访问控制日志**。
2. 在访问控制日志页面，可以查看云防火墙基于用户在互联网边界防火墙、NAT 边界防火墙、VPC 间防火墙和企业安全组间配置的访问控制规则所生成的规则命中记录日志。
3. 同时，在互联网边界防火墙、NAT 边界防火墙页面下，访问控制日志会根据入站以及出站方向生成两张规则命中列表，方便用户区分查看。

4. 在规则命中列表的右侧操作栏，单击**查看**。



5. 在命中规则详情页面，可查看针对该条规则的详细命中情况。

> **说明：**
> - 若在日志生成时间后，该规则被用户删除，则状态显示为已删除。
> - 若在日志生成时间后，该规则被用户编辑，则状态显示为已编辑。
> - 若在日志生成时间后至今，该规则未被编辑或删除，则状态显示为新增。

6. 为了进一步加快对访问控制日志的检索及过滤，可以通过单击访问源或访问目的右侧的 🔍，查看这两个 IP 地址之间的全部规则命中情况。

7. 单击页面右侧的 ⬇，可以手动下载日志，页面可以做条件筛选。每次下载限6万条记录。

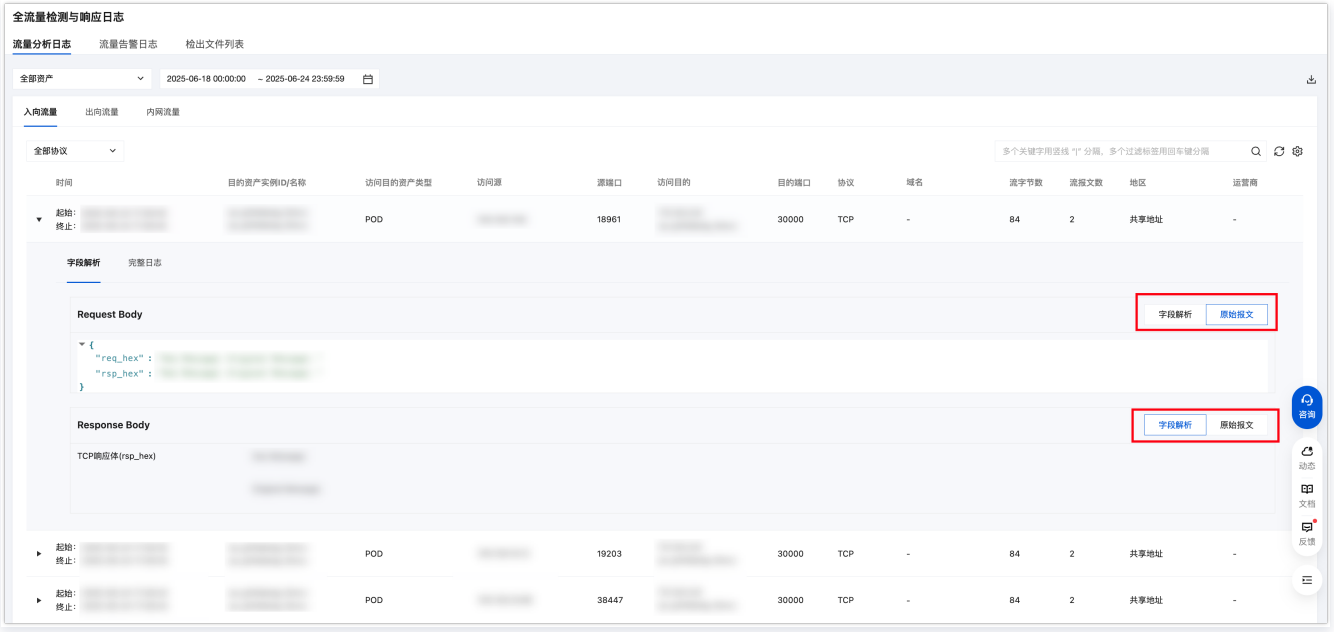
查看入侵防御日志

1. 登录 云防火墙控制台，在左侧导航栏中，选择**日志审计 > 入侵防御日志**。
2. 在入侵防御日志页面，可查看云防火墙基于“观察模式”和“拦截模式”所产生和记录的所有安全事件，有“外部入侵，主机失陷，横向移动，网络蜜罐”四个列表，分别查看入站和出站的安全事件详细情况。

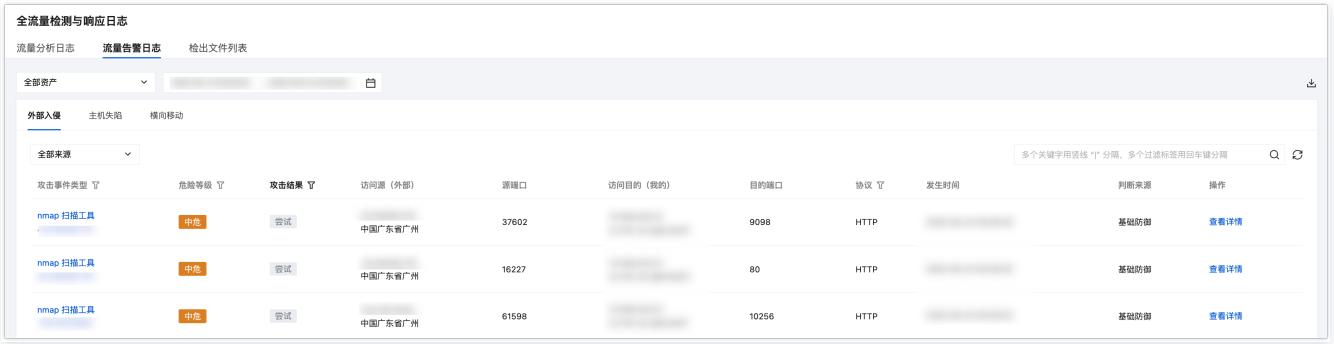
查看全流量检测与响应日志

全流量检测与响应日志包含流量分析日志、流量告警日志、检出文件列表。

1. 登录 云防火墙控制台，在左侧导航栏中，选择**日志审计 > 全流量检测与响应日志**。
2. 在全流量检测与响应日志页面，分为如下三部分：
   - 流量分析日志为全流量检测与响应的流量分析日志，可查看入向流量、出向流量、内网流量日志。

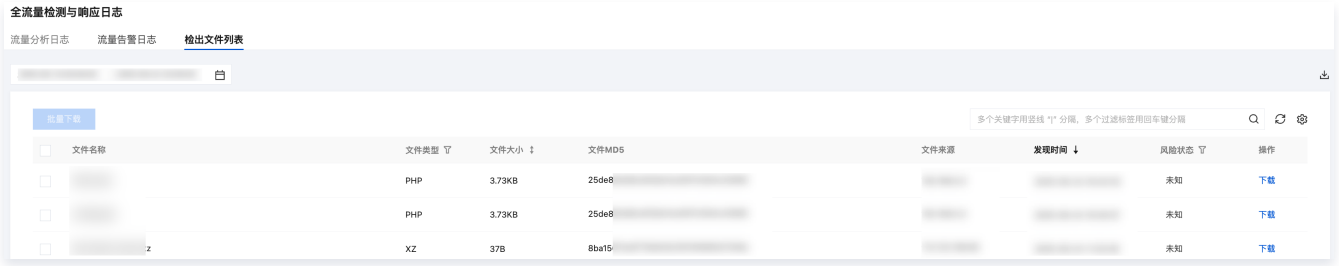


   - 流量告警日志支持查看全流量检测与响应告警的告警日志，包含外部入侵、主机失陷、横向移动，支持攻击结果筛选查询。



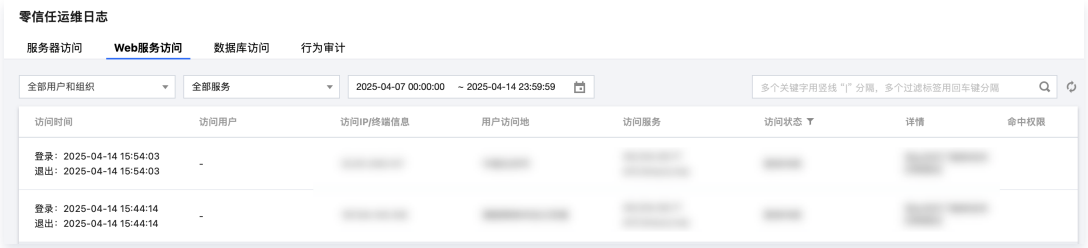
单击**查看详情**，支持查看流量告警日志详情，支持查看会话还原、完整日志及 PCAP 下载。

- 检出文件列表支持查看文件的MD5值，并可下载文件。



查看零信任运维日志

1. 登录 云防火墙控制台，在左侧导航栏中，选择**日志审计 > 零信任运维日志**。
2. 在零信任防护日志页面，可查看用户对于服务器访问、Web 服务访问、数据库访问、行为审计四个模块下的零信任运维日志，包括登录与访问服务详情。



查看流量日志

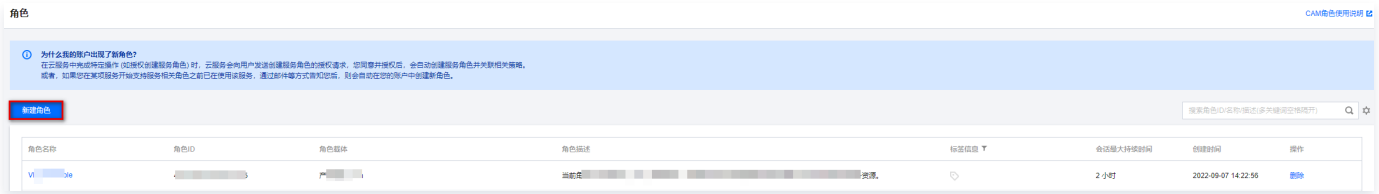
1. 登录 云防火墙控制台，在左侧导航栏中，选择**日志审计 > 流量日志**。
2. 在流量日志页面，可以查看互联网边界防火墙和 NAT 边界防火墙基于出站和入站所产生的南北向流量十元组信息，以及 VPC 间的东西向流量情况。

3. 使用资产实例名进行日志的查询和过滤。为了方便通过资产的粒度和角度去全局查看流量情况，可以在流量日志页面左上角，单击**全部资产**，在搜索下拉框使用某个资产实例名对日志进行过滤，并查询该资产的所有流量日志。

4. 为了进一步加快对日志的检索及过滤，可以通过单击访问源或访问目的右侧的 🔍，查看这两个 IP 地址之间的全部流量情况。

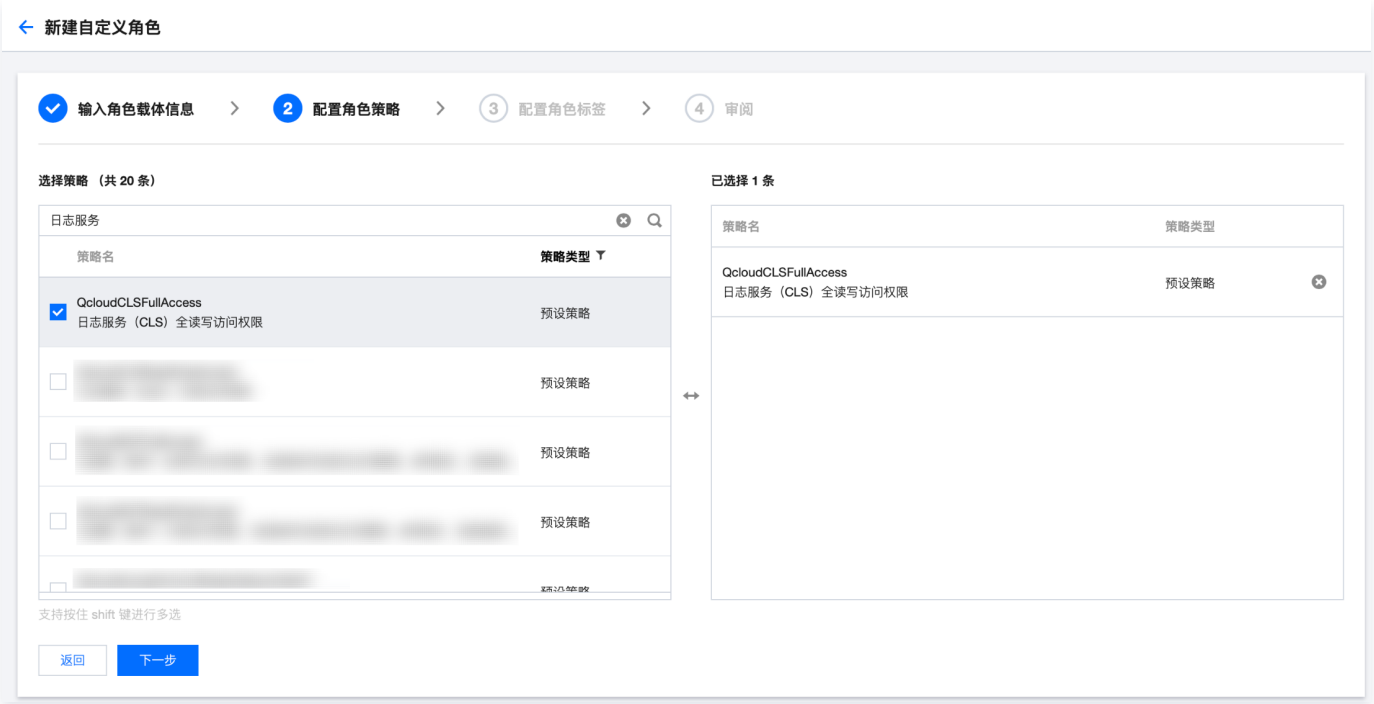
内网流量日志授权

1. 登录 访问管理控制台，在左侧导航栏中选择**角色**。
2. 在角色页面，单击**新建角色**，选择腾讯云账号，进入新建自定义角色页面。



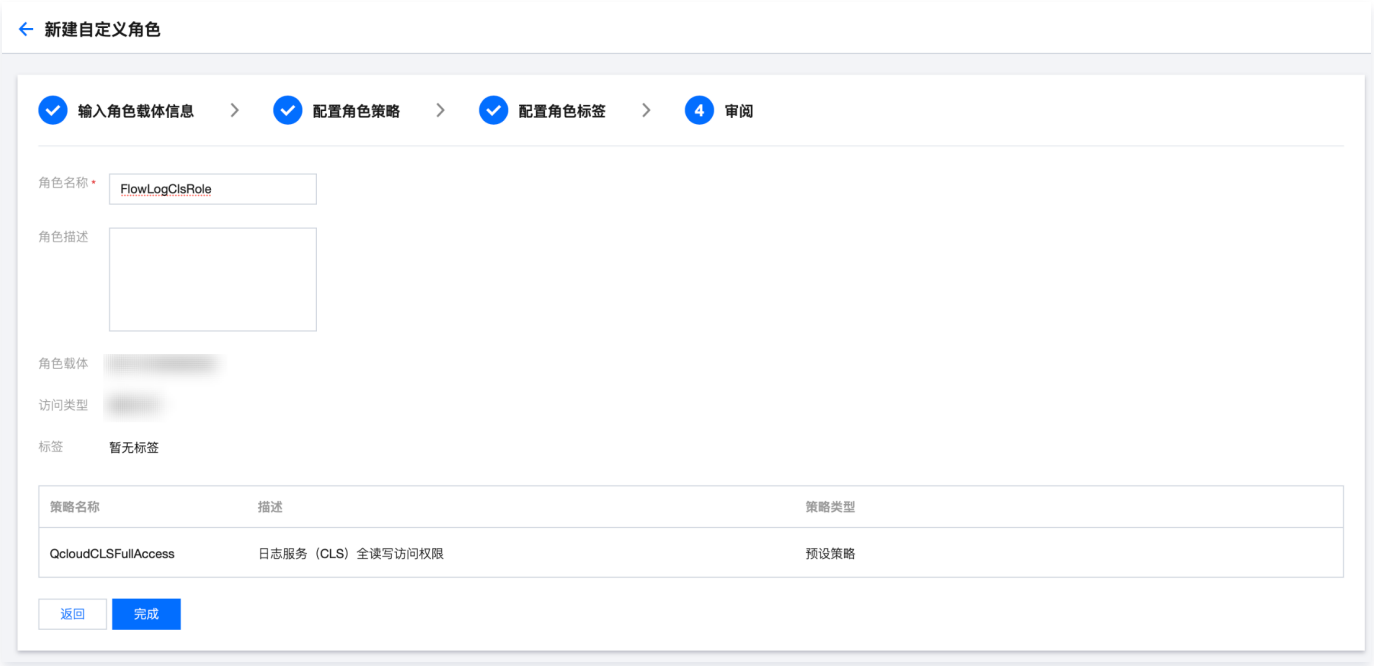
3. 在新建自定义角色页面，选择其他主账号，并输入流日志公共账号 91000000202，单击**下一步**。

4. 检索关键字“日志服务”，授权日志服务全读写权限 QcloudCLSFullAccess，单击**下一步**。



5. 配置角色标签，可以为子用户设置不同维度的标签，也可以跳过不配置。单击**下一步**。

6. 输入角色名称 FlowLogClsRole，单击**完成**，完成新建角色。



查看操作日志

1. 登录 云防火墙控制台，在左侧导航栏中，选择**日志审计 > 操作日志**。
2. 在操作日志页面，可以查看基于该账号内，用户针对安全策略以及开关页所进行的所有操作行为以及操作详情。

标签名称	标签说明
防火墙开关	记录防火墙开关情况以及用户配置实例的操作详情。
资产中心操作	记录用户对于资产中心模块所进行的操作详情。
访问控制操作	记录用户对于访问控制规则的新增/编辑和删除操作。
零信任防护操作	记录用户对于零信任防护模块所进行的操作详情。
入侵防御操作	记录用户对于入侵防御模块所进行的操作详情。
地址模板操作	记录用户对地址模板进行操作的详情。
网络蜜罐操作	记录用户对蜜罐服务、暴露探针进行的操作。
日志投递操作	记录用户日志投递操作详情。
登录日志	记录该用户全部账号的登录情况。

相关信息

如遇到日志审计相关问题，可参见 日志相关 文档。

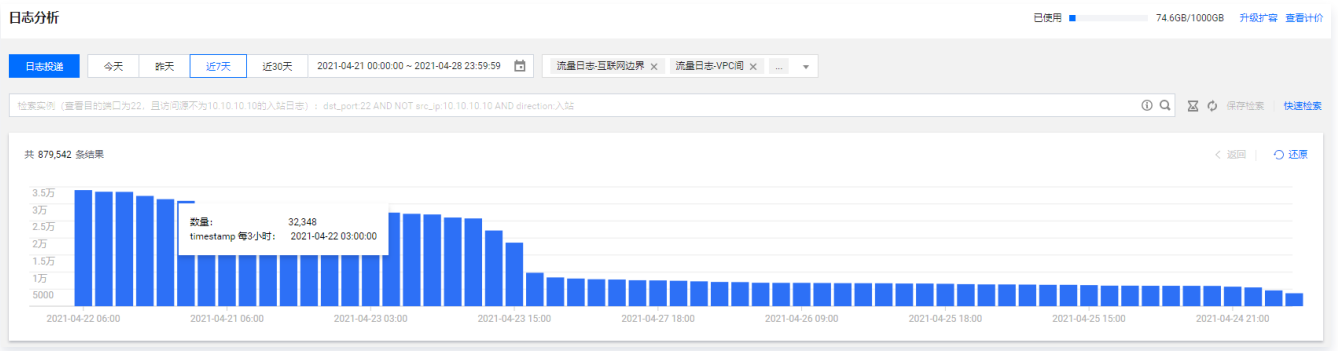
日志分析

最近更新时间：2025-01-23 17:14:12

日志分析可查看基于登录账号的云防火墙在过去6个月所存储的全部日志详情，同时日志分析支持基于检索语句的日志检索与查询，并提供报表与统计分析服务。本文档将为您介绍如何使用日志分析功能。

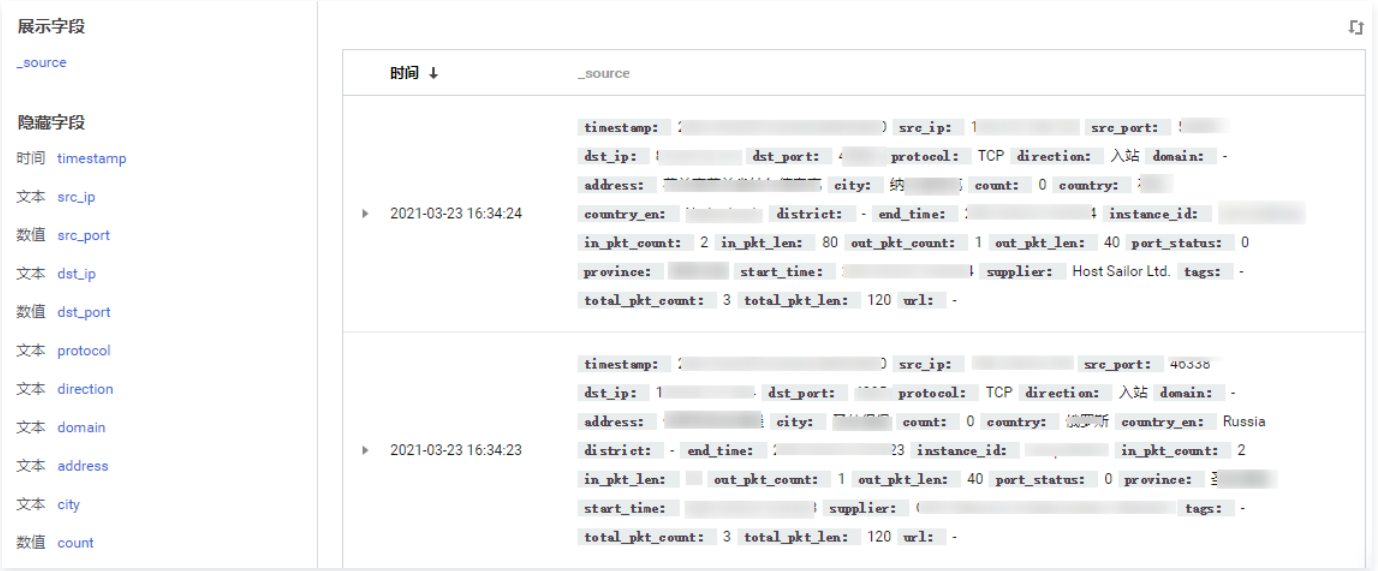
操作步骤

1. 登录 云防火墙控制台，在左侧导航栏中，单击**日志分析**，进入“日志分析”页面。
2. 为了方便对指定单位时间范围内的日志检索操作，您可以将鼠标在页面上的蓝色日志数量柱形图上滑动，快速选定时间范围，单击蓝色日志数量柱形图，可进一步对日志进行放大搜索。
   - 还原：在柱形图右上角单击**还原**，时间选择器会回到初始时间范围（今天）。
   - 切换时间选择器的选项、切换日志类型及重新输入检索框等重新出发检索的操作，都会使柱形图回归当前时间选择器范围的初始时间（今天）。



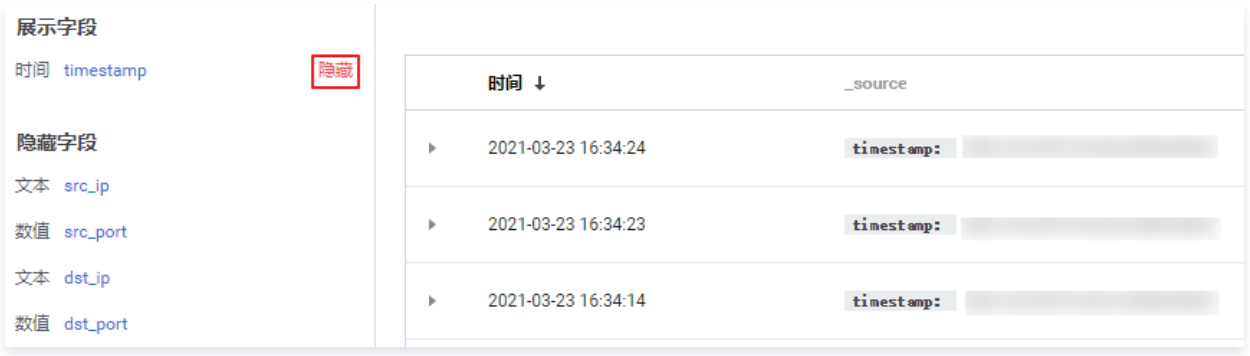
> **注意：**
> - 当日志存储容量写满后将不再写入，若需要扩大日志存储容量，单击页面右上角处的升级扩容按钮，进行容量购买。
> - 使用日志分析的用户，可支持每个自然月4次手动清空日志机会，于**通用设置 > 日志存储设置 > 日志清空次数 > 手动清空**处操作。
> - 企业版及以上用户支持自定义存储时长，于**通用设置 > 日志存储设置 > 日志存储时长 > 编辑**处操作。

3. 日志列表会根据“展示字段”模块内容，按照从上到下的顺序展示每个流量日志的字段详情。当“展示字段”中仅有 source 字段时，日志列表中展示的字段顺序将会为“隐藏字段”的顺序。



- **显示**：将鼠标移动至隐藏字段上方，在隐藏字段右侧，单击**显示**，该隐藏字段将出现在展示字段中，对应右侧日志列表将展示该字段内容。

- **隐藏**：将鼠标移动至展示字段上方，在展示字段右侧，单击**隐藏**，该隐藏字段将在展示字段中删除，对应右侧日志列表将不再展示该字段内容。



日志投递

最近更新时间：2025-04-14 16:41:32

投递至 CLS

通过日志投递功能，您可以将云防火墙日志自动投递到指定的 CLS 实例中，实现对云防火墙日志的高效存储与分析。以下为您详细介绍如何使用日志分析中的日志投递功能至 CLS。

> **说明：**
> 使用投递至 CLS，需要先开通腾讯云日志服务，了解日志服务的使用和收费模式。

背景信息

- 日志投递功能可依据不同的云防火墙日志类型，分别将其精准投递到指定的 CLS 日志主题（Log Topic）中，便于您根据日志类别进行针对性管理与分析。
- 日志投递功能支持两种网络接入方式，分别是：公网接入和腾讯云 VPC 内网接入。
  - 借助公网实现云防火墙日志向 CLS 的投递，适用于部分无法直接接入腾讯云内网的场景。
  - 通过腾讯云内部私有网络进行日志投递，在安全性和传输性能上更具优势，能有效保障数据传输的稳定性与高效性。

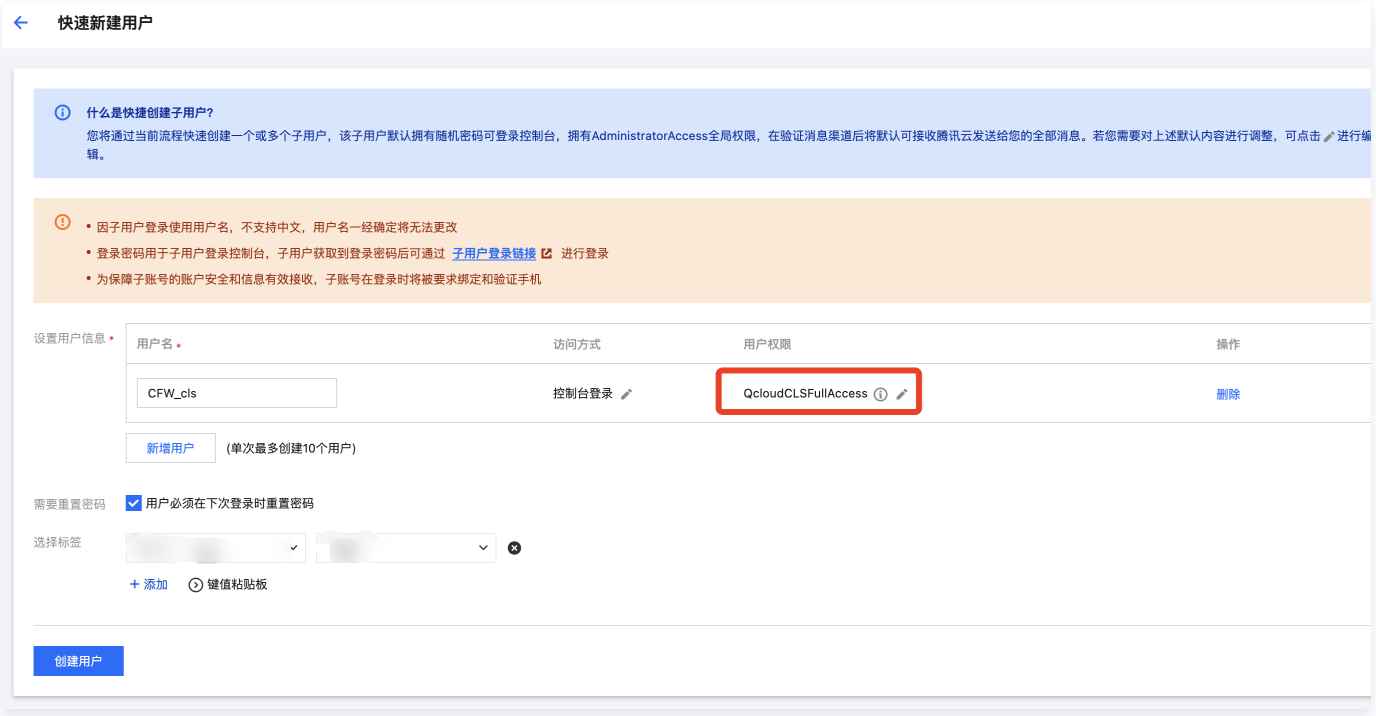
前提条件

需已开通腾讯云 CLS 服务和 云防火墙日志分析。

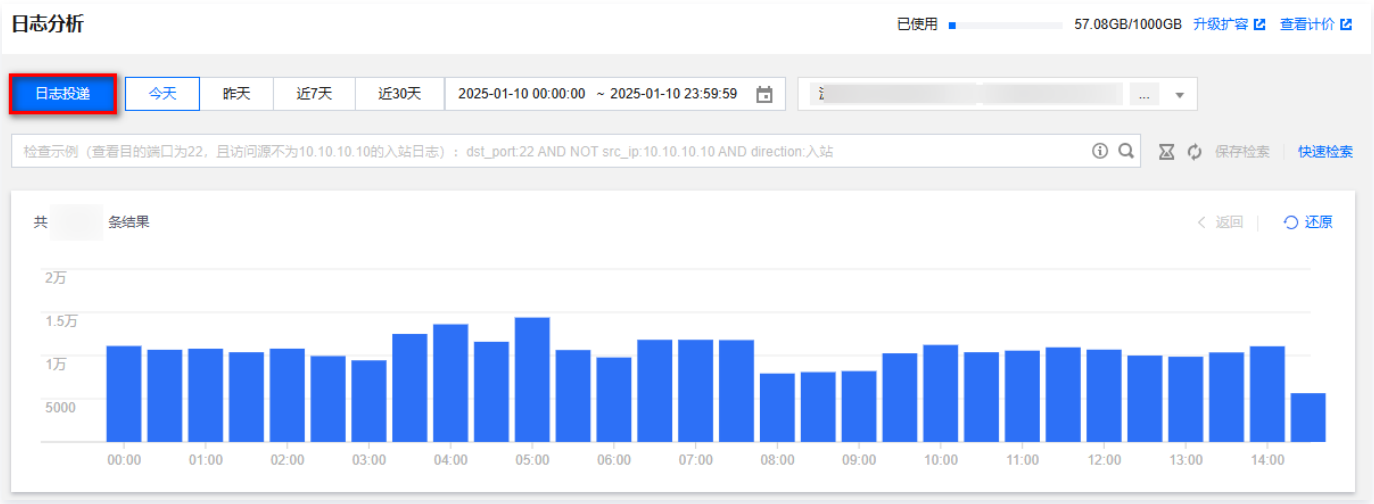
配置步骤

1. 推荐新建子账号进行日志投递，使用主账号进入 访问管理-用户列表 页面，为防火墙日志投递任务创建专属 API 调用账号，并赋予 CLS 的全读写权限 `QcloudCLSFullAccess`。

   > **说明：**
   > 使用主账号、已创建的子账号，也可以配置云防火墙日志投递。如使用子账号，需要确保子账号已有 `QcloudCLSFullAccess` 权限，没有的情况下可以在 访问管理-用户列表页面 为子账号授权 `QcloudCLSFullAccess`。



2. 登录 云防火墙控制台，在左侧导航栏中，单击**日志分析**。
3. 在日志分析页面，单击**日志投递** > **投递至 CLS**。



4. 在 投递至CLS页面，单击配置 CLS 投递的**编辑**，填写 SecurityID 和 SecurityKey 进行身份认证，单击保存，完成 CLS 投递的配置。

> **说明：**
> Security ID 可以在 访问控制-API 密钥管理 获取，Security Key 在创建账号时获得。

5. 在投递至 CLS 页面，找到**投递开关**选项，将开关按钮从**关闭**状态切换为**打开**状态。

完成以上步骤后，腾讯云防火墙的日志将成功投递至 CLS，您可以在 CLS 控制台中进一步管理和分析接收到的日志数据，以便更好地监控网络安全状况和进行相关的运维操作。

投递至 Ckafka

通过日志投递功能，您可以将云防火墙日志自动投递到指定的 Ckafka 实例中。接下来将为您介绍，如何使用日志分析中的日志投递功能。

背景信息

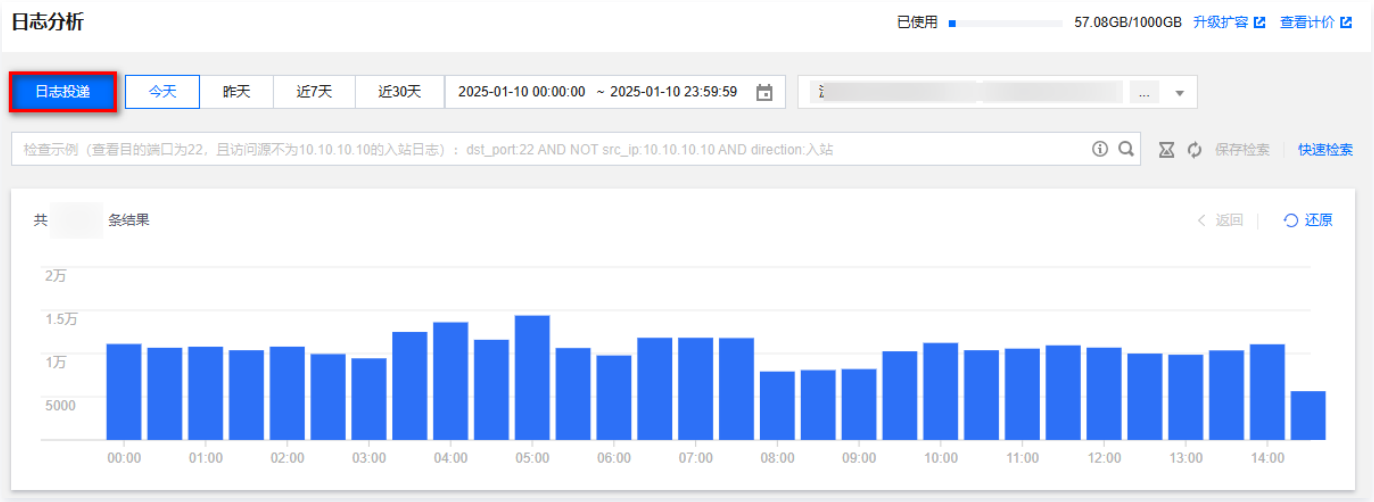
- 日志投递功能可以按照不同的云防火墙日志类型，分别投递到指定的 Ckafka topic 中。
- 日志投递功能支持两种网络接入方式，分别是：公网域名接入和支撑环境接入。
  - 公网域名接入是通过公网进行日志投递的。
  - 支撑环境接入是通过腾讯云内网进行日志投递，性能更高。

前提条件

- 需已 购买腾讯云消息队列 Ckafka 实例 和 云防火墙日志分析，按照云防火墙带宽来配置 Ckafka 实例的带宽规格。
- 根据 消息队列 Ckafka 文档 指引，联系 腾讯云客服 开通“公网域名接入”或“支撑环境接入”白名单。
- 仅支持使用一个消息队列 Ckafka 账号进行日志投递。

配置步骤

1. 登录 云防火墙控制台，在左侧导航栏中，单击**日志分析**。
2. 在日志分析页面左上角，单击**日志投递**，默认进入投递至 Kafka 页面。



3. 在投递至 Kafka 页面，进行初始配置。

   3.1 选择网络接入方式分为：公网域名接入及支撑环境接入。

   - **方式1**：选择公网域名接入，选择消息队列实例和公网域名，并输入所选消息队列实例的用户名和密码。

- **方式2：选择支撑环境接入，支撑环境接入指您在腾讯云已选购可以与 Ckafka 结合使用的产品，并选择消息队列实例和 IP 端口。**

3.2 选择网络接入方式后，可以在日志投递页面绑定 Ckafka topic。

> **说明：**
> 日志投递功能支持多种云防火墙日志类型的投递，不同类型的日志需要投递到不同的 Ckafka topic 中。每个 Ckafka topic 只能被一个云防火墙日志类型所绑定。

3.3 配置完成后，单击**确定**，将提示配置日志投递成功，表示日志投递已经配置成功。

4. 初始化配置完成后，即可查看日志投递详情。

- **基本信息**：展示了 Ckafka 实例的基本信息。

  > **注意：**
  > 您需要关注“健康状态”字段，当提示“不健康”时，需要单击**查看监控**，查看 Ckafka 服务是否异常，或者是否配额不足。

- **日志投递开关**：用于控制指定的日志类型，启动或停止日志投递任务。
  - 方式1：您可以在各项日志类型的右侧“投递开关”列，通过“开关”按钮单独控制日志投递任务。
  - 方式2：使用批量操作，目前支持**全部启动**和**全部停止**两种操作。
- **重新绑定 Ckafka topic**：在日志类型的右侧的操作栏，单击**编辑**进行单独配置，可以重新选择指定 Ckafka 实例中，未被其他防火墙日志类型绑定的 Ckafka topic。

  > **说明：**
  > 每个 Ckafka topic 只能被一个云防火墙日志类型所绑定。

- **查看监控**：在日志类型的右侧的操作栏，单击**查看监控**，会跳转至消息队列 Ckafka 控制台的监控页面，您可以查看网络流量、峰值带宽、消息条数、磁盘占用等情况。
- **重新配置**：在日志类型列表上方，单击**重新配置**，将会允许您重新选择投递的消息队列实例、网络接入方式以及用户名/密码。

  > **注意：**
  > 重新配置，会中断当前的投递进程。

日志字段
日志细类字段

最近更新时间：2024-05-17 15:14:11

日志类型 ID	日志类型名称
CFWRuleAcl	访问控制日志-互联网边界
CFWRuleVpcAcl	访问控制日志-NAT、VPC 防火墙
HoneyPotHost	入侵防御日志-网络蜜罐-主机日志
HoneyPotNetwork	入侵防御日志-网络蜜罐-网络日志
BlockList	入侵防御日志-拦截列表日志
IdsLog	入侵防御日志-虚拟补丁、基础防御日志
TiLog	入侵防御日志-威胁情报日志
BaseLineLog	入侵防御日志-安全基线日志
CFWOnline	流量日志-互联网边界
CFWNetflowVpc	流量日志-VPC
CFWNetflowNat	流量日志-NAT
CFWNetflowFI	流量日志-内网流量
CFWOperateLogAll	操作日志
CFWOperateRemoteOM	零信任防护日志-远程运维登录
CFWOperateWebAccess	零信任防护日志-Web 服务访问

版权所有：腾讯云计算（北京）有限责任公司

访问控制类型

最近更新时间：2025-04-14 16:41:32

字段标识	字段类型	字段名称	字段描述	参考值	细分类型	备注
src_ip	string	源 IP	-	192.168.0.1	CFWRuleAcl、CFWRuleVpcAcl	-
dst_ip	string	目的 IP	-	192.168.0.1	CFWRuleAcl、CFWRuleVpcAcl	-
src_port	uint16	源端口	-	22	CFWRuleAcl、CFWRuleVpcAcl	-
dst_port	uint16	目的端口	-	22	CFWRuleAcl、CFWRuleVpcAcl	-
protocol	string	协议	-	tcp	CFWRuleAcl、CFWRuleVpcAcl	-
info	string	URL 信息	HTTP 命中日志的 URL	domain/test.php	CFWRuleAcl	-
direction	int8	方向	制定规则的流量方向	出站	CFWRuleAcl、CFWRuleVpcAcl	-
detail	string	规则告警描述（附带规则描述）	告警详情信息	-	CFWRuleAcl、CFWRuleVpcAcl	-
rule_info	string	规则告警详情（用于关联规则）	-	-	CFWRuleAcl	-
strategy	string	策略	规则执行的动作策略		CFWRuleAcl、CFWRuleVpcAcl	-
time	int64	事件	命中规则的时间	-	CFWRuleAcl、CFWRuleVpcAcl	-
appid	string	appid	账号 appid	-	CFWRuleAcl	-
instance_id	string	受害者相关资产 ID	受害者相关资产 ID	-	CFWRuleAcl、CFWRuleVpcAcl	-
uuid	string	原始告警日志唯一 ID	原始告警日志唯一 ID	-	CFWRuleAcl	-
uid	int64	规则唯一 ID	规则唯一 ID（内部使用）	-	CFWRuleAcl	-
insert_time	int64	日志插入时间	记录此日志的时间	-	CFWRuleAcl、CFWRuleVpcAcl	-

版权所有：腾讯云计算（北京）有限责任公司

mode	uint8	防火墙属性	0：旁路 1：串行	-	CFWRuleAcl	-
type	uint8	协议 TYPE 类型	协议 TYPE： 1：TCP 3：HTTP	-	CFWRuleAcl	-
fw_type	string	防火墙类型	规则所属的防火墙类型	NAT 边界防火墙	CFWRuleAcl、CFWRuleVpcAcl	-
timestamp	string	时间戳	当前时间	-	CFWRuleAcl、CFWRuleVpcAcl	-
fws_id	string	引擎实例 ID		cfwnat-fd7f678e	CFWRuleVpcAcl	-
nat_ins_name	string	NAT 的实例名称	-	-	CFWRuleVpcAcl	-
log_type	uint8	日志类型（内部使用）	当前日志类型固定值：5	-	CFWRuleVpcAcl	-
dst_vpc	string	受害者资产 VPCID	-	-	CFWRuleVpcAcl	当前日志字段为空值时，当前字段默认隐藏
fws_name	string	引擎实例名称	-	-	CFWRuleVpcAcl	-
src_vpc	string	攻击者资产 VPCID	-	-	CFWRuleVpcAcl	当前日志字段为空值时，当前字段默认隐藏
region	string	区域	-	-	CFWRuleVpcAcl	-
dst_domain	string	外联域名	外联的域名信息	-	CFWRuleVpcAcl	-
l7proto	string	七层协议名称	-	DNS、SMTP、HTTP	CFWRuleVpcAcl	-
src_vpc_name	string	访问源 VPC 名称	-	-	CFWRuleVpcAcl	当前日志字段为空值时，当前字段默认隐藏
dst_vpc_name	string	访问目的 VPC 名称	-	-	CFWRuleVpcAcl	当前日志字段为空值时，当前字段默认隐藏
ew_ins_id	string	VPC 墙实例 ID	-	-	CFWRuleVpcAcl	-
ew_ins_name	string	VPC 墙实例名称	-	-	CFWRuleVpcAcl	-
src_ins_id	string	访问源资产 ID	-	-	CFWRuleVpcAcl	当前日志字段为空值时，当前字段默认隐藏
dst_ins_id	string	访问目的资产 ID	-	-	CFWRuleVpcAcl	当前日志字段为空值时，当前字段默认隐藏
src_ins_name	string	访问源实例名称	-	-	CFWRuleVpcAcl	当前日志字段为空值时，当前字段默认隐藏
dst_ins_na	string	访问目的实	-	-	CFWRuleVpcA	当前日志字段为空值时，当前

me		例名称			cl	字段默认隐藏

零信任防护日志

最近更新时间：2024-05-17 15:14:11

字段标识	字段类型	字段名称	字段描述	细分类型
service	string	运维服务类型	SSH/RDP 等	CFWOperateRemoteOM、CFWOperateWebAccess
src_ip	string	源 IP	-	CFWOperateRemoteOM、CFWOperateWebAccess
src_port	uint16	源端口	-	CFWOperateRemoteOM、CFWOperateWebAccess
dst_ip	string	目的 IP	-	CFWOperateRemoteOM、CFWOperateWebAccess
dst_port	uint16	目的端口	-	CFWOperateRemoteOM、CFWOperateWebAccess
appid	string	appid	-	CFWOperateRemoteOM
user	string	运维用户的名称	当 ywid 存在时，使用的是对应的名称，否则为空	CFWOperateRemoteOM
corp_id	string	企业微信企业 ID	以企业用户去登录时的企业 ID	CFWOperateRemoteOM
msg	string	登录状态	登录成功等	CFWOperateRemoteOM
session	string	会话 ID	会话 ID	CFWOperateRemoteOM
ywid	int64	运维用户 ID	运维表的运维 ID	CFWOperateRemoteOM
filename	string	回放文件名	回放文件名	CFWOperateRemoteOM
login_type	int64	登录状态码	登录状态码，和 msg 对应，代表登录状态	CFWOperateRemoteOM
start_time	int64	会话的开始时间	-	CFWOperateRemoteOM、CFWOperateWebAccess
end_time	int64	会话的结束时间	-	CFWOperateRemoteOM、CFWOperateWebAccess
login_failed_type	int64	登录失败的原因	-	CFWOperateRemoteOM
address_en	string	访问地址	-	CFWOperateRemoteOM
req_uri	string	会话访问的 URL	-	CFWOperateWebAccess
pay_load	string	会话请求载荷	-	CFWOperateWebAccess
access_type	int64	登录状态	-	CFWOperateWebAccess
access_time	string	登录时间	-	CFWOperateWebAccess
request_time	string	会话请求时间	-	CFWOperateWebAccess
user_id	string	登录的用户 ID	运维 ID	CFWOperateWebAccess
user_corp_id	string	登录的企业微信企业 ID	以企业用户去登录时的企业 ID	CFWOperateWebAccess
user_type	string	用户类型	企业微信用户，普通用户	CFWOperateWebAccess
wx_name	string	微信名称	微信名称	CFWOperateWebAccess
openid	string	微信的openid	-	CFWOperateWebAccess
src_region	string	源区域	-	CFWOperateWebAccess

版权所有：腾讯云计算（北京）有限责任公司

dst_instance_id	string	访问的实例 ID	-	CFWOperateWebAccess
http_cookie	string	请求 cookie 信息	会话 cookie	CFWOperateWebAccess

入侵防御日志

最近更新时间：2024-05-17 15:14:11

字段标识	字段类型	字段名称	字段描述	参考值	细分类型
instance_id	string	受害者相关资产 ID	-	-	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
time	int64	告警发生时间	-	-	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
src_ip	string	源 IP	-	192.168.0.1	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
dst_ip	string	目的 IP	-	192.168.0.1	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
src_port	int64/int	源端口	-	-	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
dst_port	int64/int	目的端口	-	-	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
direction	int64	方向	• 0：出站 • 1：入站 • TCP 协议告警：为会话方向 • 非会话协议：为流量方向	-	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
protocol	string	协议	-	TCP	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
strategy	string	告警动作	告警的处置动作 • 0：观察 • 1：阻断 • 2：放行 • 3：欺骗	0	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
strategy_res	string	告警动作标识 ID	-	strage_alert	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog
event_name	string	攻击事件类型	-	Log4j2漏洞利用	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog

版权所有：腾讯云计算（北京）有限责任公司

eventname_res（event_name_res）	string	攻击事件类型标识 ID	-	log4j2_exploit	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog
dst_domain	string	外联域名	-	-	HoneyPotHost、HoneyPotNetwork、BlockList、TiLog、BaseLineLog
level	string	告警级别	告警的严重程度	严重	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
level_res	string	告警级别标识 ID	-	level_serious	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog
level_int	int	告警级别数字	-	5	HoneyPotHost、HoneyPotNetwork
address	string	攻击 IP 的所处城市	-	日本东京都东京	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
address_en	string	攻击 IP 的所处城市	-	Tokyo，Japan	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog
insert_time	int64	告警入库时间	-	2023/1/1 0:00:00	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
service_id	string	网络蜜罐 ID	-	-	HoneyPotHost、HoneyPotNetwork
type	string	告警子类型标识	-	ti	HoneyPotHost、HoneyPotNetwork、TiLog、BaseLineLog
sub_source_type	string	告警子类型	告警分类，包括：虚拟补丁、基础防御、封禁列表、网络蜜罐等	虚拟补丁	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
sub_source_type_res	string	告警子类型标识 ID	告警子类型标识 ID，source_virtualpatch 虚拟补丁，source_basicrule 基础防御等	source_virtualpatch	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog
payload	string	攻击 payload	攻击流量的载荷信息	-	HoneyPotHost、HoneyPotNetwork、IdsLog、TiLog
cmdline	string	执行命令	网络蜜罐主机事件，蜜罐内执行的敏感命令	bash -c ifconfig execve /bin/bash|m=100755|o=0:0	HoneyPotHost

template_id	string	网络蜜罐模板 ID	-	-	HoneyPotHost
docker_id	string	网络蜜罐唯一 ID	-	-	HoneyPotHost、HoneyPotNetwork
proc_chan	string	进程树	网络蜜罐主机事件进程树	bashP{	HoneyPotHost
kill_chain	string	攻击链	攻击链，告警事件所处攻击阶段	漏洞利用	HoneyPotHost、HoneyPotNetwork
kill_chain_res	string	攻击链标识 ID	-	kill_chain_exploit	HoneyPotHost、HoneyPotNetwork
event_id	string	告警 ID	-	-	HoneyPotHost、HoneyPotNetwork
exe	string	执行文件路径	-	/sbin/ifconfig	HoneyPotHost
probe_id	string	探针 ID	-	probe-id	HoneyPotHost、HoneyPotNetwork
service_type	string	网络蜜罐类型	网络蜜罐类型	SSH 蜜罐	HoneyPotHost、HoneyPotNetwork
service_type_res	string	网络蜜罐类型标识 ID	-	ssh_honeypot	HoneyPotHost、HoneyPotNetwork
script_name	string	网络蜜罐剧本名称	-	-	HoneyPotHost、HoneyPotNetwork
log_source	string	数据来源	VPC 间防火墙的告警和内网蜜罐告警值为 move 蜜罐主机告警值为 host 蜜罐公网告警值为 network	move	HoneyPotHost、HoneyPotNetwork、IdsLog
login_user	string	攻击登录用户	-	[root, 1qaz!QAZ]	HoneyPotHost、HoneyPotNetwork
visible_tag	int	可见性	-	-	HoneyPotHost、HoneyPotNetwork
timestamp	string	告警时间戳	-	2023-01-01T00:00:00+08:00	HoneyPotHost、HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
ti_type	string	关联情报威胁类型标签（告警中自带）	-	["SSH蜜罐攻击","常规网络爆破","暴力破解"]	HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
ti_type_en	string	关联情报威胁类型标签（告警中自带）	-	["SSH honeypot attack","General network cracking","Brute force"]	HoneyPotNetwork、BlockList、IdsLog、TiLog
ti_white	string	白名单标签（告警中自带）	-	情报白名单	HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog
ti_white_res	string	白名单标签（告警中自带）标识 ID	-	intelligence_allowlist	HoneyPotNetwork、BlockList、IdsLog、TiLog、BaseLineLog

src_country	string	源国家	源 IP 的所处国家	美国	BlockList、IdsLog、TiLog、BaseLineLog
src_country_en	string	源国家-英文	源 IP 的所处国家-英文	United States of America	BlockList、IdsLog、TiLog
dst_country	string	目的国家	目的 IP 的所处国家	美国	BlockList、IdsLog、TiLog、BaseLineLog
dst_country_en	string	目的国家-英文	目的 IP 的所处国家-英文	United States of America	BlockList、IdsLog、TiLog
attack_vector	string	攻击利用方法	-	code-exec	IdsLog
attack_count	int	告警数量	-	-	IdsLog
nat_ip	string	NAT的 IP	NAT 的公网 IP 地址	8.8.8.8	IdsLog、TiLog、BaseLineLog
nat_port	int	NAT的端口	NAT 的公网端口	-	IdsLog、TiLog、BaseLineLog
fws_id	string	防火墙 ID	-	-	IdsLog
fw_type	string	防火墙类型	防火墙类型，包括： • vpc：VPC 间防火墙 • nat：NAT 防火墙 • sg：企业安全组 • 空：互联网边界	nat	IdsLog
src_vpc	string	攻击者资产 VPCID	-	-	IdsLog
dst_vpc	string	受害者资产 VPCID	-	-	IdsLog
src_ins_id	string	攻击者相关资产 ID	-	-	IdsLog
dst_ins_id	string	受害者相关资产 ID	-	-	IdsLog
nat_ins_id	string	NAT 的实例 ID	-	-	TiLog、BaseLineLog
nat_ins_name	string	NAT 的实例名称	-	-	TiLog

版权所有：腾讯云计算（北京）有限责任公司

流量日志

最近更新时间：2025-02-12 10:02:42

字段标识	字段类型	字段名称	字段描述	参考值	细分类型	备注
appid	string	appid	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
instance_id	string	资产实例 ID	-	-	CFWOnline、CFWNetflowNat	-
src_ip	string	源 IP	-	192.168.0.1	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
dst_ip	string	目的 IP	-	192.168.0.1	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
src_port	uint16	源端口	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
dst_port	uint16	目的端口	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
protocol	string	协议	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
direction	int8	方向	流量方向	出站	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	sd-wan
dst_domain	string	访问目的域名	-	-	CFWOnline、CFWNetflowNat	-
in_pkt_count	uint64	入向包个数	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
in_pkt_len	uint64	入向包大小	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
out_pkt_count	uint64	出向包个数	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
out_pkt_len	uint64	出向包大小	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
total_pkt_count	uint64	总包个数	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
total_pkt_len	uint64	总包大小	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
ti_tag	string	关联情报标签（告警中自带）	-	-	CFWOnline、CFWNetflowNat	-
start_time	int64	会话的开始时间	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
end_time	int64	会话的结束时间	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	-
supplier	string	运营商	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
supplier_en	string	运营商-英文	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan

版权所有：腾讯云计算（北京）有限责任公司

src_country	string	源国家	源 IP 的所处国家	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
src_country_en	string	源国家-英文	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
dst_country	string	目的国家	目的 IP 的所处国家	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
dst_country_en	string	目的国家-英文	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
src_province	string	源省份	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
src_province_en	string	源省份-英文	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
dst_province	string	目的省份	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
dst_province_en	string	目的省份-英文	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
src_city	string	源城市	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
dst_city	string	目的城市	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
district	string	地区	-	-	CFWOnline、CFWNetflowNat	-
address	string	详细地址	• 入站为源详细地址 • 出站为目的详细地址	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
address_en	string	详细地址-英文	• 入站为源详细地址-英文 • 出站为目的详细地址-英文	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
src_lat	float32	源维度	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
dst_lat	float32	目的维度	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
src_lon	float32	源经度	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
dst_lon	float32	目的经度	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat	sd-wan
insert_time	int64	日志入库时间	-	-	CFWOnline、CFWNetflowNat	-
count	uint64	告警数量	-	-	CFWOnline	-
url	string	七层 URL	-	-	CFWOnline	-
domain_flag	uint8	是否存在域名	• 1：存在 • 0：不存在	-	CFWOnline	-
port_status	uint8	端口状态	• 1：打开 • 0：关闭	-	CFWOnline	-

bot_flag	uint8	保留字段	-	-	CFWOnline	-
mode	uint8	防火墙属性	• 1：串行 • 0：旁路	-	CFWOnline	-
argus_ip	uint32	保留字段	-	-	CFWOnline	-
tcp_flag	uint8	TCP 标记	• 1：OUTSyn • 2：OUTRst • 3：OutSynAck • 4：OUTFin • 5：INSyn • 6：INRst • 7：INSynAck • 8：InFin	-	CFWOnline	-
timestamp	string	统一时间戳	-	-	CFWOnline、CFWNetflowVpc、CFWNetflowNat、CFWNetflowFl	sd-wan
cvm_id	string	保留字段	-	-	CFWNetflowVpc	-
ew_ins_id	string	VPC 防火墙实例 ID	-	-	CFWNetflowVpc	-
fws_id	string	VPC 防火墙边 ID	-	-	CFWNetflowVpc、CFWNetflowNat	-
fws_name	string	VPC 防火墙名称	-	-	CFWNetflowVpc	-
log_type	uint8	日志类型（内部使用）	当前日志类型固定值：2	-	CFWNetflowVpc	-
if_pair_key	string	保留字段	-	-	CFWNetflowVpc	-
uuid	int64	原始告警日志唯一 ID	-	-	CFWNetflowVpc	-
flow_id	int64	内部字段	-	-	CFWNetflowVpc	-
src_vpc	string	攻击者资产 VPCID	-	-	CFWNetflowVpc	-
dst_vpc	string	受害者资产 VPCID	-	-	CFWNetflowVpc	-
dst_vpc_name	string	目的 VPC 名称	-	-	CFWNetflowVpc	-
src_vpc_name	string	源 VPC 名称	-	-	CFWNetflowVpc	-
retans	int8	是否有重传	• 1：重传 • 0：没重传	-	CFWNetflowVpc、CFWNetflowNat	-
timeout	int64	会话持续时间	-	-	CFWNetflowVpc、CFWNetflowNat	-
src_ins_id	string	攻击者相关资产 ID	-	-	CFWNetflowVpc、CFWNetflowFl	-
dst_ins_id	string	受害者相关资产 ID	-	-	CFWNetflowVpc、CFWNetflowFl	-

版权所有：腾讯云计算（北京）有限责任公司

src_ins_name	string	源资产名称	-	-	CFWNetflowVpc	-
dst_ins_name	string	目的资产名称	-	-	CFWNetflowVpc	-
is_out	int8	SDWAN 防火墙访问公网标记	• 1：访问公网 • 0：正常访问	-	CFWNetflowVpc	sd-wan
ti_tag_en	string	攻击者 IP 情报标签-英文	-	-	CFWNetflowNat	-
fw_type	string	告警子类型	-	-	CFWNetflowNat	-
fw_region	string	防火墙所在地域	-	-	CFWNetflowNat	-
nat_ip	string	NAT 的 IP	NAT 的 IP 地址	-	CFWNetflowNat	-
nat_port	uint16	NAT 的端口	-	-	CFWNetflowNat	-
if_id	string	网卡 ID	-	-	CFWNetflowFl	-
action	string	告警动作	告警处置动作	拦截，放行	CFWNetflowFl	-

操作日志

最近更新时间：2024-05-17 15:14:11

字段标识	字段类型	字段名称	细分类型	备注
level	string	危险等级	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
operator	string	操作者	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
result	string	操作结果	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
fw_type	string	防火墙类型	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
action	string	防火墙开关-操作行为 资产中心操作-操作行为 访问控制操作-操作行为 零信任防护操作-操作行为 入侵防御操作-操作类别 地址模板操作-操作行为 网络蜜罐操作-操作行为 通用设置操作-操作行为	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
opt_type	string	操作日志大类	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
detail	string	防火墙开关-操作详情 资产中心操作-操作详情 访问控制操作-操作详情 零信任防护操作-操作详情 入侵防御操作-操作行为 地址模板操作-模板描述 网络蜜罐操作-操作详情 通用设置操作-操作详情	CFWOperateLogAll、CFWOperateWebAccess	当前日志字段为空值时，当前字段默认隐藏
time	string	发生时间	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
app_id	string	租户唯一 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
info	string	访问控制操作-规则描述 入侵防御操作-操作详情 地址模板操作-操作详情	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
longitude	float32	源经度	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
address	string	源城市	CFWOperateLogAll、CFWOperateRemoteOM	当前日志字段为空值时，当前字段默认隐藏
district	string	源城市区县	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
more_info	string	补充信息	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
rule	string	规则列表	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏

版权所有：腾讯云计算（北京）有限责任公司

instance_region	string	资产实例地域	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
public_ip	string	蜜罐公网 IP	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
remote_type	string	操作类型 通用设置操作-日志类型	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
services	string	蜜罐详细信息	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
template_id	string	蜜罐模板 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
region	string	资产地域	CFWOperateLogAll、CFWOperateWebAccess	当前日志字段为空值时，当前字段默认隐藏
instance_id	string	相关资产 ID	CFWOperateLogAll、CFWOperateRemoteOM	当前日志字段为空值时，当前字段默认隐藏
asset_type	string	资产分类	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
addr_name	string	模板名称	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
base_type	string	基线类型	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏
timestamp	string	告警时间戳	CFWOperateLogAll、CFWOperateRemoteOM、CFWOperateWebAccess	当前日志字段为空值时，当前字段默认隐藏
level_res	string	危险等级标识 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
action_res	string	操作行为标识 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
detail_res	string	操作详情标识 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
rulelist	string	规则列表	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
appid	string	appid	CFWOperateLogAll、CFWOperateWebAccess	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
instance_region_res	string	资产实例地域标识 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
rule_res	string	规则列表标识 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
natinsid	string	NAT 的实例 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
remote_type_res	string	操作类型标识 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段

版权所有：腾讯云计算（北京）有限责任公司

detail_id	string	操作详情资产 ID	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段
base_type_res	string	安全基线类型	CFWOperateLogAll	当前日志字段为空值时，当前字段默认隐藏；仅国际站展示当前字段

通知及设置相关

最近更新时间：2025-06-30 10:49:22

订阅消息中心

云防火墙默认采用非订阅推送方式，通知账号参照通知设置中的账号配置。云防火墙会自动识别登录过云防火墙控制台的账号并加入到可选列表中。

1. 登录 云防火墙控制台，在左侧导航中，单击**通知设置**。
2. 在通知设置页面，对防火墙的推送通知进行设置。如果您需要调整为订阅类推送或启用消息中心的配置，可单击**消息中心订阅设置**中的**开关**。

注意：

启用消息中心后，通知设置中所有告警类型的告警对象将失效，详情以 消息中心 设置为准。

配置通知设置

在 通知设置页面，可以配置一些防火墙常见的告警和通知。

通知类型	通知内容	支持配置项
安全告警通知	云防火墙支持对告警中心的安全事件告警进行短信、站内信和微信通知，在控制台可以配置对象和告警来源	• 支持配置“腾讯云安全”微信服务号告警 • 支持按照告警类型触发通知
带宽告警通知	我们为您提供三级阶梯带宽告警，当防火墙带宽达到您设定的阈值百分比，即会触发对所选账户短信、站内信和微信的告警通知	支持按照防火墙类型区分不同梯级告警
全流量检测与响应通知	当带宽规格超量或单机带宽过载会进行站内信、短信的告警通知	• 支持配置带宽规格超量设置，包含超量告警通知、超量处置通知、超量恢复通知 • 支持单机带宽过载设置，包含过载处置通知、过载恢复通知
存储告警通知	我们为您提供二级阶梯存储告警，当防火墙存储达到您设定的阈值百分比，即会触发对所选账户短信、站内信和微信的告警通知	支持配置梯级告警
容灾告警通知	当您的 NAT 边界防火墙或 VPC 防火墙触发 BYPASS 时，即会触发所选账户短信，站内信和邮件的告警通知	-
新增暴露面告警通知	当检测到您的账号新增勾选的暴露面类型时，即会触发所选账户短信，站内信和邮件的告警通知	支持按暴露面类型触发通知
企业安全组变动通知	当检测到您的账号企业安全组发生变动时，无论您是否开启自动下发，我们均会为您推送相关通知	-

自动化任务异常通知	当检测到您的自动化任务出现异常时，我们会为您推送相关通知	-
系统日志推送通知	当您产生新的系统日志时，我们将会按照您的设定进行通知	支持按系统日志事件类型触发通知

通用设置

在 通用设置页面，通用设置整合了一些常用的使用配置。

设置项名称	设置项描述	注意事项
云内 IP 封禁设置	云防火墙封禁 IP 时支持根据恶意 IP 类型自动下发对应企业安全组规则至 DMZ 区，请勿手动修改对应参数模板和企业安全组规则	互联网旁路防火墙无法封禁云内 IP，串行和 NAT 防火墙支持，建议优先使用。
日志存储设置	企业版及以上用户可以修改日志存储类型和存储时长，每 2 个月仅可修改 1 次。我们会为您自动删除过期日志。您也可以手动清空日志，但请注意每个用户每个自然月仅有 4 次机会	日志设置变更后存量日志将不会生效，仅限自编辑时刻起新增日志生效。例如您将日志存储时间从180天修改为90天，则存量日志仍会存储180天，新增日志则会存储90天。
访问控制规则设置	访问控制规则列表中，每次添加、插入、导入控制规则时，设置规则的启用状态	-
蜜罐自动重建设置	网络蜜罐中，如果蜜罐失陷，可选择是否自动重建蜜罐和间隔时间	-
标签设置	云防火墙无资源属性，仅支持对账号所属计费资源添加标签，您可以在此修改标签值。	-

常用工具
地址模板

最近更新时间：2024-05-17 15:49:31

地址模板为用户提供更方便快捷的方式批量管理常用地址。用户可以在地址模板中创建 IP 模板、域名模板或协议端口模板；模板可应用于访问控制规则中，方便管理和运维。本文将为您介绍如何在地址模板中批量管理地址，同时用户可以将建立好的模板匹配访问控制中的相关规则，更方便管理。

功能入口

1. 登录 云防火墙控制台，在左侧导航中，单击**常用工具**。
2. 在常见工具页面，单击**地址模板**的**前往配置**。

3. 在地址模板页面，用户可以新建及编辑模板，并可在访问控制页面添加规则时，直接调用模板，减少操作频次。

新建模板

1. 在地址模板页面，单击**新建模板**。
2. 在新建地址模板弹窗中，选择**模板类型**。
   - IP 地址模板：仅包含 IP 地址或 CIDR，支持 IP 地址范围。
   - 域名模板：仅包含域名类地址，支持泛域名。
   - 协议端口模板：协议和端口的组合，按照四层协议和七层协议进行区分，端口支持单个端口、组合端口或端口段。

版权所有：腾讯云计算（北京）有限责任公司

3. 输入地址模板名称、IP 地址、描述，单击**确定**，即完成新建地址模板。

> **说明**
> - 输入单条地址时，用回车换行。
> - 同时输入多个地址时，请在粘贴前确保地址格式用英文逗号分隔，以便系统识别。
> - 输入重复地址，后台将自动合并。
> - 单个地址模板最多支持同时添加500条地址，填写规范及内容详见控制台。

编辑模板

地址模板创建完成后，可以在左侧的地址模板列表中查询；用户可以在已经建立好的模板列表中，添加、删除及修改对应分类的地址。

1. 在地址模板页面，单击目标地址模板右侧操作列的**编辑**。
2. 在编辑地址模板弹窗中，选择需编辑的 IP 地址进行修改或删除，或在搜索框搜寻需修改的 IP 地址，进行操作，单击**确定**保存。

> **说明：**
> 模板类型不支持编辑，如需修改请 删除模板 重新新建。

删除模板

1. 在地址模板页面，单击目标地址模板右侧操作列的**删除**。

> **注意：**
> - 如存在关联规则，请前往 访问控制页面，删除对应联系规则。
> - 删除操作不可恢复，建议先备份当前模板。

2. 在确认删除弹窗中，单击**确定**，即可删除该规则。

使用地址模板

在 访问控制页面，可以单击**添加规则**或找到需要修改的规则单击右侧**编辑**，选择使用地址模板。

> **说明：**
> - 用地址模板配置的访问规则对模板内的全部地址生效。
> - 地址模板仅支持配置互联网边界规则、NAT 边界规则、内网间规则及 DNS 规则，不支持配置企业安全组。
> - 地址模板数量有限，请合理规划及利用。

IP 地址模板或域名模板

在访问控制规则中，您可以在**访问源**或**访问目的**中选择**地址模板**，列表下拉菜单中将列出支持配置的 IP 地址模板或域名模板。

> **说明：**
> 模板类型的选择与协议相关，请按照对应访问控制规则的提示填写。

协议端口模板

在访问控制规则中，您可以在**端口协议类型**中选择**协议端口模板**，列表下拉菜单中将列出支持配置的协议端口模板。

> **说明：**
> 模板类型的选择与访问源或访问目的配置的形式相关，请按照对应访问控制规则的提示填写。

规则备份

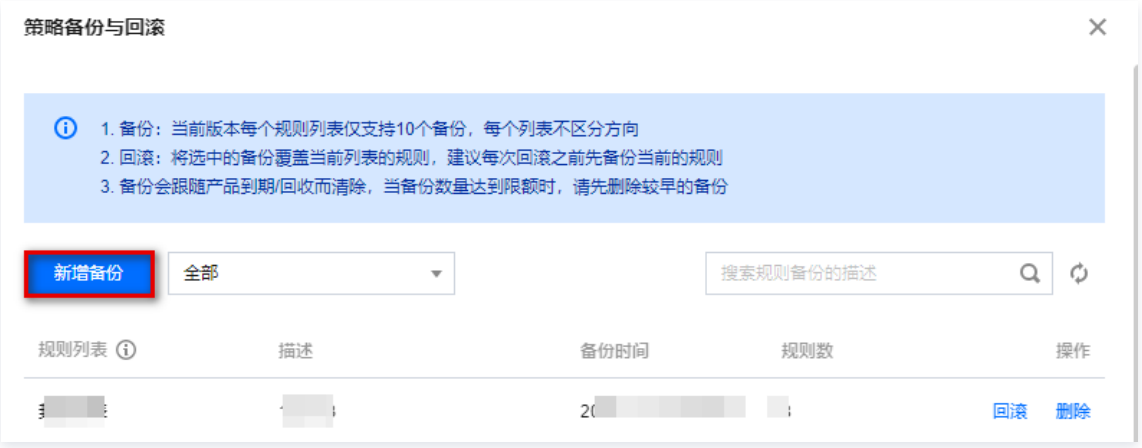
最近更新时间：2024-05-17 15:57:11

在修改访问控制规则时，支持对现有的规则进行备份，以及支持对不同防御状态的规则回滚。

新增备份

1. 登录 云防火墙控制台，在左侧导航中，单击**访问控制**。
2. 在访问控制页面，单击右上角的**规则备份**，弹出策略备份与回滚弹窗。

3. 在策略备份与回滚窗口，单击**新增备份**。



4. 选择备份的规则列表，填写备注，单击**确定**，完成新增规则备份。

回滚备份

1. 在 访问控制页面，单击右上角的**规则备份**，弹出策略备份与回滚弹窗。
2. 选择已备份的规则，单击**回滚**。

3. 在“确认使用备份回滚规则列表”弹窗中，单击**确定**，即可将备份的规则回滚，覆盖当前的规则列表。

> **注意**
> 规则回滚操作将会覆盖对应的规则列表，现有的策略将会被删除，为了保证数据安全，建议先将当前列表进行备份处理。

删除备份

1. 在 访问控制页面，单击右上角的**规则备份**，弹出策略备份与回滚弹窗。
2. 选择已备份的规则，单击**删除**。

3. 在“确认删除”弹窗，单击**确定**，即可删除已备份好的规则。

> **注意**
> 规则备份删除后无法找回/恢复，请谨慎操作。

自动化助手

最近更新时间：2024-10-17 20:59:31

自动化助手是为企业版及以上版本用户提供自动化指令和定时指令的运维工具，用户可以自行编排指令实现自动化运维。

功能入口

1. 登录 **云防火墙控制台**，在左侧导航中，单击**常用工具**。
2. 在常见工具页面，单击**自动化助手**的**前往配置**。

3. 在自动化助手页面，用户可以新建及编排自动化任务，实现定时启停访问控制规则、定时忽略分类告警等功能。

添加自动化任务

1. 在自动化助手页面，单击**添加任务**。
2. 在新建自动化任务弹窗中，填写自动化任务名称。

3. 单击任务对象右侧的**点击选择**，您可以通过**分类选择**或者**自定义选择**的形式，选择自动化任务想要关联的任务对象，单击**确定**。

> **说明：**
> 当前版本支持选择的对象类型包括**所有访问控制规则列表**及**待处置的入侵防御告警**。

4. 单击**添加动作**，添加想要执行的任务动作，支持设置临时任务或者周期任务及执行时间。多个动作将会按照执行顺序和时序依次执行；单击**复制**，可添加执行动作数，最多支持添加10条。

> **说明：**
> 当前版本支持的动作如下：
> - 访问控制规则类型：启用规则、停用规则。
> - 待处置入侵防御告警：忽略告警。

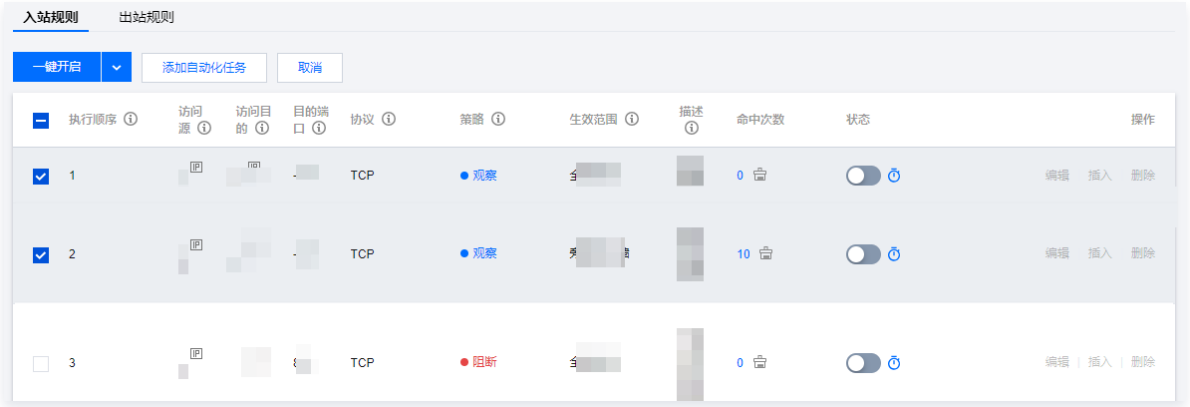
5. 单击**提交**，即可在任务列表中查询已配置的自动化任务及任务状态。

快捷添加自动化任务

您可以从访问控制规则列表中快速添加任务，以下以互联网边界规则举例。

1. 登录 云防火墙控制台，在左侧导航中，单击**访问控制 > 互联网边界规则**。
2. 在互联网边界规则页面，单击**批量操作**。

3. 勾选想要执行自动化任务的规则，单击**添加自动化任务**。



4. 在新建自动化任务窗口中，填写任务名称，单击**添加动作**，配置其他参数，单击**提交**。

编辑自动化任务

1. 在 常用工具页面，单击**自动化助手的前往配置**。

2. 在自动化助手页面，找到想要编辑的任务，单击**编辑**。

3. 在编辑自动化任务弹窗中，支持编辑任务名称、任务类型、任务动作、执行时间，也可以进行复制或者删除任务，单击**提交**保存。

> **注意：**
> 请注意任务对象变动后（如编辑、删除等）将不再执行自动化任务。

删除任务

1. 在 常用工具页面，单击**自动化助手的前往配置**。

2. 在自动化助手页面，找到想要删除的任务，单击**删除**。

3. 在确认删除窗口中，单击**确认**，即可删除该任务。

查询执行记录

在自动化任务关联对象的 操作日志 中，可以查阅到账号名为“自动化任务”的操作记录。

网络抓包工具

最近更新时间：2024-10-17 20:59:31

网络抓包工具为企业版及以上版本用户提供获指定 IP 和端口的网络数据包、分析数据包内容的工具，帮助您定位网络故障和分析攻击行为，从而识别出网络通信的安全风险。

功能入口

1. 登录 云防火墙控制台，在左侧导航中，单击**常用工具**。
2. 在常见工具页面，单击**网络抓包工具**的**前往配置**。

3. 在网络抓包工具页面，用户可以针对 NAT 边界防火墙和 VPC 间防火墙的流量进行抓包并下载分析。

新建抓包任务

1. 在网络抓包工具页面，单击**新建抓包任务**。

2. 在新建抓包任务弹窗中，配置相关参数，单击**开始抓包**。

> **注意：**
> 请确认您的抓包对象已开启对应防火墙开关，否则将无法抓取对应流量。

3. 等待抓包任务完成后，单击**下载**，下载抓包结果。

> **注意：**
> 抓包完成后请及时下载抓包文件，有效期为 3 天。

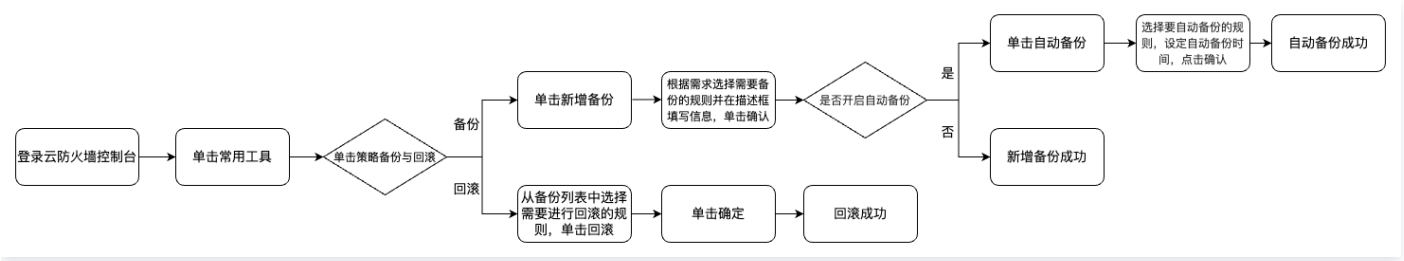
4. 可以使用 Wireshark 等网络抓包软件打开抓包结果，以便进行进一步的分析。

策略备份与回滚

最近更新时间：2025-01-25 11:30:52

为应对可能出现的误操作、策略变更需求或紧急故障恢复场景，特提供策略备份与回滚功能，确保您的网络防护策略稳定可靠。
通过策略备份与回滚，可以快速撤销近期的修改，使互联网边界防火墙、NAT 边界防火墙、VPC 边界防火墙、企业安全组的策略配置回到之前保存的状态。

流程图

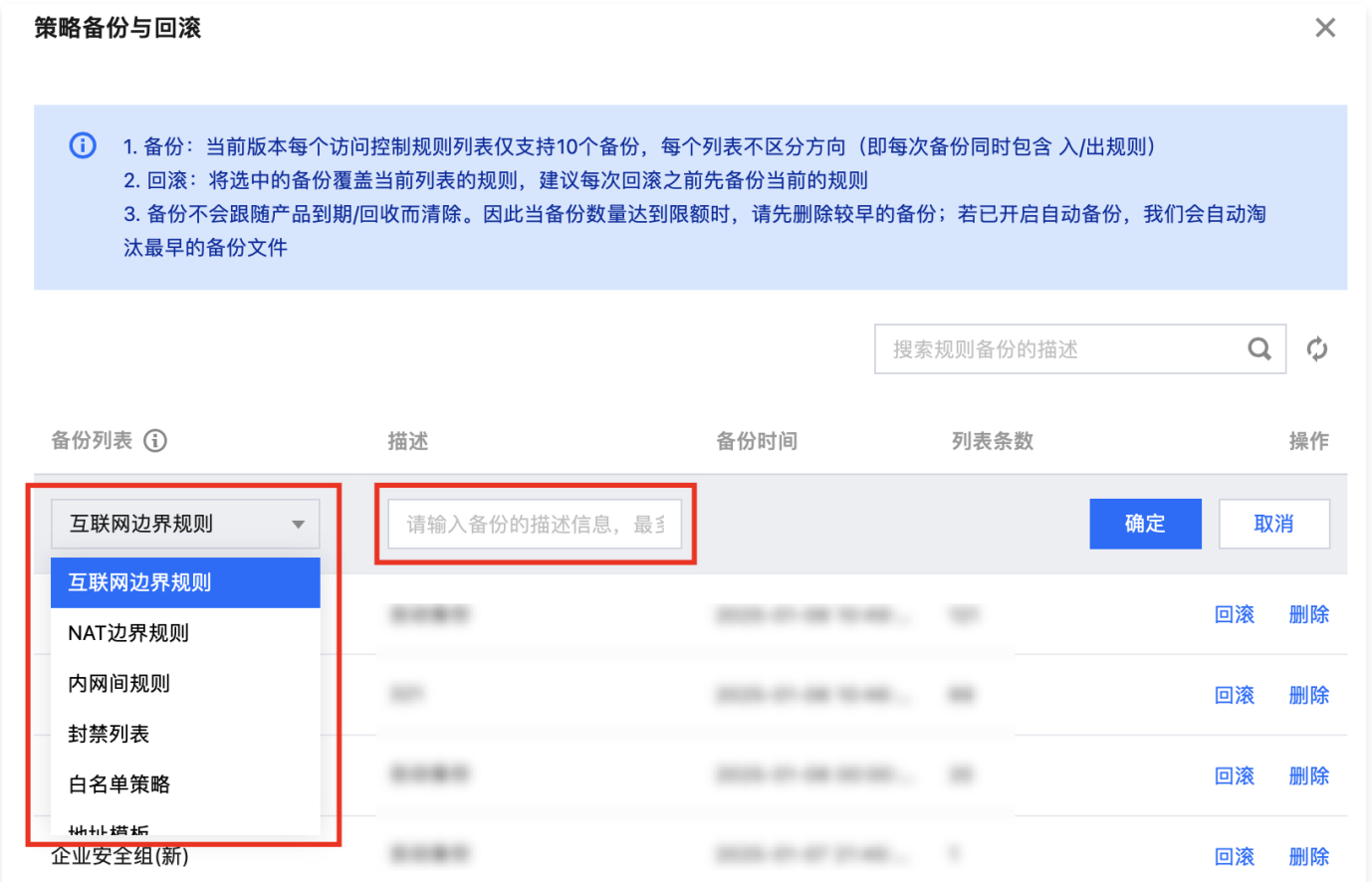


策略备份

1. 登录 云防火墙控制台，在左侧导航中，单击**常用工具**。
2. 在常用工具页面，单击**策略备份与回滚**的**前往配置**。

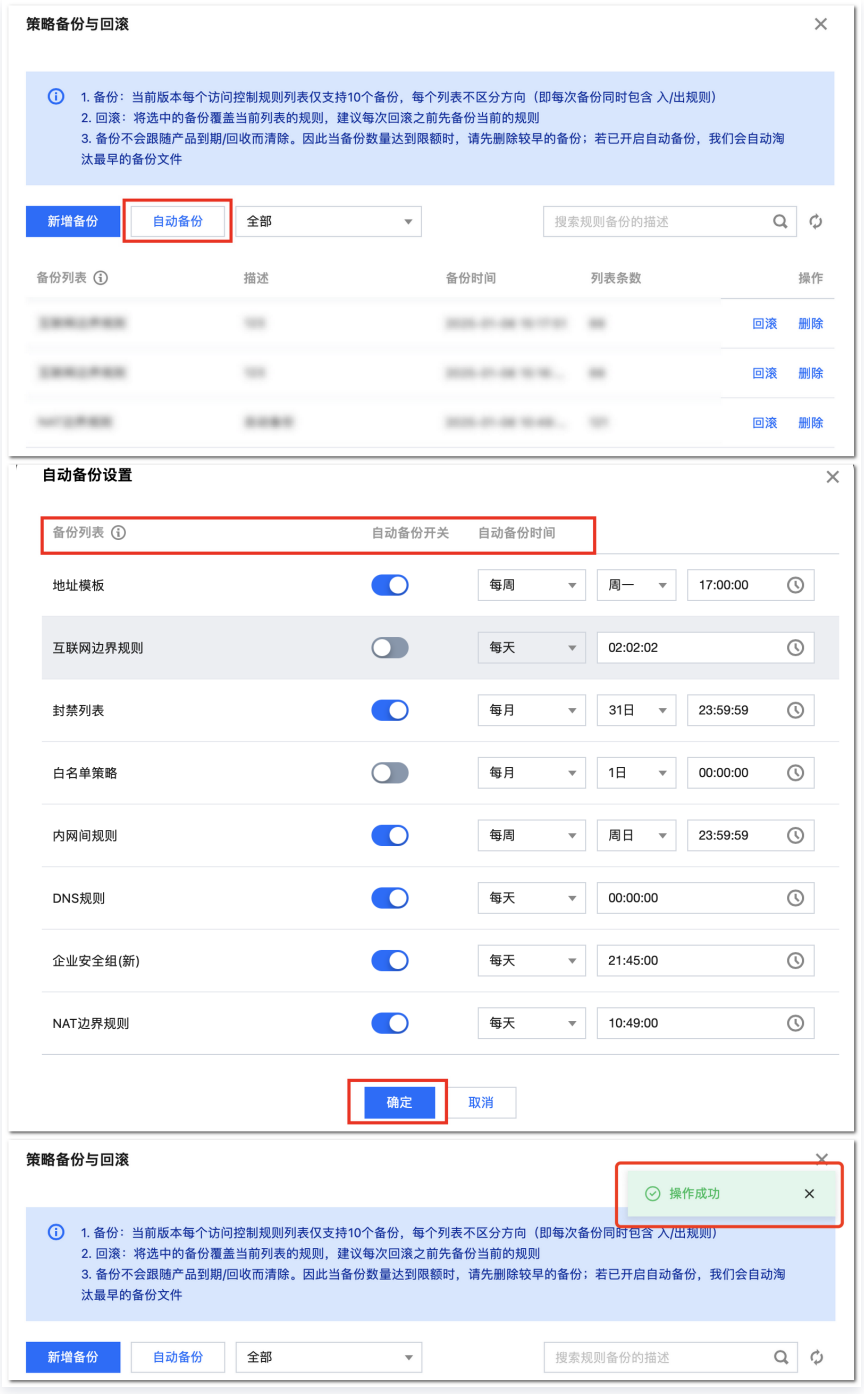
3. 在策略备份与回滚页面，单击**新增备份**。

4. 展开备份列表选项框，系统会列出当前可备份的规则列表，您可根据需求选择。同时，为方便后续识别备份用途，请在**描述**栏填写清晰、简洁的描述信息。



5. 完成上述规则选择与描述信息填写后，单击**确定**，系统将立即启动备份程序，备份完成后，会有‘备份成功’的提示信息，告知您此次备份已顺利完成并妥善存储。

6. 系统还可以按照需求定时**自动备份**您选定的规则。单击**自动备份**，系统会列出可备份的规则列表，选择需要开通自动备份配置的规则并为自动备份设定合适的时间，完成规则和时间的选择后，核对信息无误后，单击**确定**，系统将按照您设定的要求启动自动备份任务。



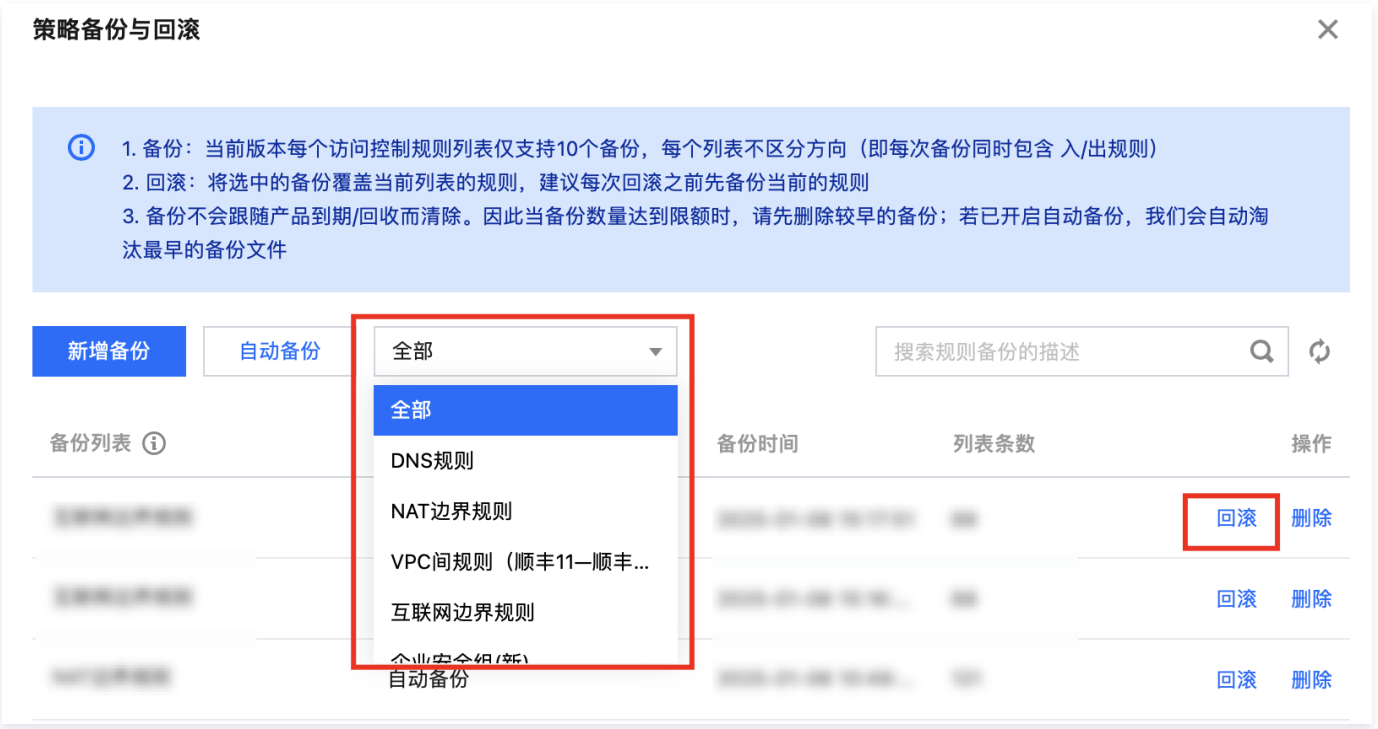
策略回滚

> **注意：**
> 使用选中的策略备份进行回滚操作将会覆盖对应的策略列表，现有的策略将会被删除，为了保证数据安全，建议先将当前列表进行 备份处理 。

1. 登录 云防火墙控制台 ，在左侧导航中，单击**常用工具**。
2. 在常用工具页面，单击**策略备份与回滚**的**前往配置**。

3. 在策略备份与回滚页面，弹窗里包括已备份的所有规则资源、描述和备份时间。

4. 下拉**选项框**找到需要进行回滚的规则，单击**回滚**。



5. **单击确定，系统立即开始将备份的规则覆盖当前规则列表。**

使用场景

场景类型		策略详情
策略备份	定期备份	按固定周期备份防火墙策略，有助于留存网络防护策略各阶段状态。后续回溯策略演变、合规审计，或对比不同阶段策略优劣时，能快速获取资料依据。例如：企业每季度内部网络安全审查，依靠定期备份可清晰展现季度间防火墙策略调整走向与重点。
	重大业务变更前	企业上线新业务系统、拓展网络区域、大规模调整服务器架构前，务必进行策略备份。新策略实施若出现影响原有业务访问、引发网络延迟、暴露安全漏洞等问题，可迅速还原备份策略，避免业务长时间中断受损。例如：电商企业在 “双 11” 购物狂欢节前，对服务器进行扩容并调整防火墙策略，若提前备份，即使新策略出现意外，也能快速回滚，保障购物节期间网络交易的顺畅。
	人员交接场景	在网络安全管理团队成员更替时，提前备份好策略，能够减少因人员变动带来的工作延误与风险。同时，备份策略也可作为新成员后续策略调整的参考基准，确保策略修改的连贯性与合理性。

策略回滚	误操作后	由于操作失误，如误删重要规则、错误配置访问权限，导致部分业务无法正常访问或出现安全隐患时，策略回滚功能可立即将策略恢复到误操作前的正确状态，保障业务正常运行。例如：管理员清理过期规则误删在用关键业务访问规则，回滚前一天备份策略就能快速修复。
	策略调整测试失败后	企业因业务发展或应对新安全威胁调整优化防火墙策略，测试中若出现与现有网络架构不兼容、无法阻挡新型攻击、影响业务性能等状况，利用回滚功能还原到调整前稳定状态，重新评估测试方案，规避失败调整带来的损失。例如：金融企业测试新入侵检测策略后发现误报率高影响效率，回滚原策略再深入研究改进。
	遭受网络攻击或故障后	企业网络遇恶意攻击致防火墙策略被篡改，或因系统故障（如硬盘损坏、软件崩溃）造成策略文件丢失、损坏，回滚功能可助企业迅速恢复到此前可靠策略配置，降低损失，为排查修复争取时间。例如：企业深夜遭 DDoS 攻击，策略被恶意修改，回滚前一天备份策略快速恢复防护，同时技术人员紧急响应查源修复。

版权所有：腾讯云计算（北京）有限责任公司