NAT 网关

公网 NAT 网关操作指南

产品文档

腾讯云

文档目录

公网 NAT 网关操作指南
修改 NAT 网关配置

最近更新时间：2024-01-05 15:11:59

NAT 网关创建后，您可以对其属性进行修改。

1. 登录 NAT 网关控制台。

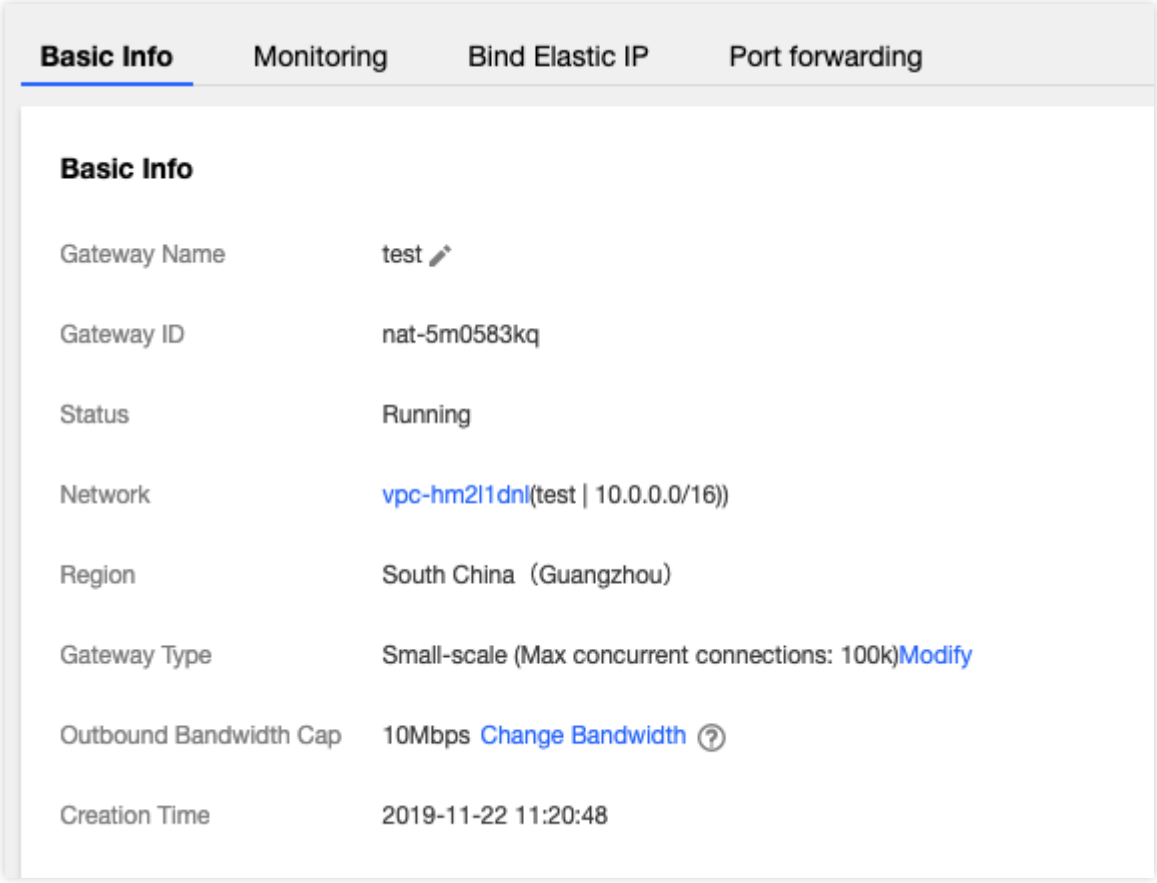
2. 在列表中单击需要修改的 NAT 网关 ID 进入详情页，在详情页可以完成如下操作。

修改网关的自定义名称。

修改网关类型，更改后实时设定，实时生效（变更类型不会中断原网络连接）。

修改出带宽上限。

添加标签，通过标签可进行权限管理。



管理 NAT 网关的弹性公网 IP

最近更新时间：2024-01-05 15:11:59

创建 NAT 网关后，您可以对网关的弹性公网 IP 进行管理，下面将为您详细介绍管理方法。

操作步骤

1. 登录 NAT 网关控制台。
2. 在列表中单击网关 ID 进入详情页。
3. 选择**关联弹性公网 IP** 标签页，在该页面可以查看 NAT 网关上绑定的 EIP 信息，也可以对 NAT 网关的 EIP 进行管理。

绑定弹性公网 IP

说明：

当一个 NAT 网关绑定多个弹性公网 IP 时，系统会自动做负载均衡。

当前仅支持绑定已有弹性公网 IP，不支持新建。需要先去 公网 IP 控制台 创建。

1. 单击弹性公网 IP 页签上方的**绑定弹性公网 IP**。
2. 在**选择 IP**下拉框中选择需要绑定的弹性公网 IP，然后单击**确定**选中一个或者多个弹性公网 IP。
3. 单击**确定**完成绑定。

调整弹性公网 IP 的带宽

1. 在对应弹性公网 IP 所在行的操作栏中，单击**调整带宽**。
2. 在**调整带宽**弹窗中调整目标带宽，然后单击**确定**

解绑弹性公网 IP

说明：

当 NAT 网关上只有一个弹性公网 IP 时，不支持解绑操作。

1. 在对应弹性公网 IP 所在行的操作栏中，单击**解绑**。
2. 在**确认解绑该弹性公网 IP** 弹窗中，单击**确定**，完成解绑。

配置指向 NAT 网关的路由

最近更新时间：2024-01-05 15:11:59

创建 NAT 网关后，需要配置路由规则，将子网流量指向 NAT 网关。
本文提供两种操作方式，您可以根据自己的需要选择任一操作方式。
方式一：从 **NAT 网关**控制台开始操作
方式二：从**路由表**控制台开始操作

操作步骤

方式一：从 NAT 网关控制台开始操作

1. 登录 NAT 控制台。
2. 在 NAT 实例列表中，单击目标 NAT 实例所在行的私有网络 ID。
3. 在私有网络详细信息中，单击**子网**。
4. 在子网列表中，选择需要访问公网的子网所在行的路由表 ID。
5. 在路由表基本信息页面，单击**+新增路由策略**。
6. 在**新增路由**弹框中，输入目的端（目的公网对应的 IP 地址段）、下一跳类型选择** NAT 网关**、下一跳选择已创建的 NAT 网关 ID。
7. 单击**创建**完成以上配置后，关联此路由表的子网内的云服务器访问公网的流量将指向该 NAT 网关。

方式二：从路由表控制台开始操作

1. 登录 私有网络控制台，在左侧目录中单击**路由表**。
2. 在路由表列表中，单击需要访问公网的子网所关联的路由表 ID 进入详情页。
3. 在路由表基本信息页面，单击**+新增路由策略**。
4. 在**新增路由**弹框中，输入目的端（目的公网对应的 IP 地址段）、下一跳类型选择 **NAT 网关**、下一跳选择已创建的 NAT 网关 ID。
5. 单击**创建**完成以上配置后，关联此路由表的子网内的云服务器访问公网的流量将指向该 NAT 网关。

管理 SNAT 规则

最近更新时间：2024-01-05 15:11:59

当 NAT 网关绑定多个 EIP 时，可以通过 创建 SNAT 规则，为不同业务分组的云服务器指定访问公网的 EIP。
例如，当 NAT 网关绑定了 EIP1、EIP2、EIP3、EIP4 等多个 EIP 时，则系统会在绑定的所有 EIP 中自动做负载均衡访问公网。如果将 EIP1、EIP2、EIP3 加入 SNAT 地址池，则系统使用 SNAT 地址池中的 EIP 访问公网，且自动在 SNAT 地址池中的 EIP 做负载均衡，没有配置 SNAT 规则的云服务器可以通过 NAT 上绑定的所有 EIP 访问公网。
说明：
当 CVM 实例负载激增时，1个 EIP 可能无法支撑巨大的访问量，可选择配置多个 EIP 分担访问量。
NAT 网关支持将同一个 EIP 同时用于配置 SNAT 规则和端口转发规则，端口转发规则的详细信息请参考 管理端口转发规则。
本文介绍如何创建和管理 SNAT 规则。

SNAT 规则限制

当 NAT 网关解关联 EIP 时，若该 EIP 为 SNAT 规则的唯一 EIP，则同时删除此条 SNAT 规则；若该 EIP 为此 SNAT 规则的非唯一 EIP，则 SNAT 规则中删除此 EIP。
SNAT 规则中使用的子网不存在时，联动删除该 SNAT 规则。
SNAT 规则中使用的云服务器不存在时，联动从 SNAT 规则中删除该云服务器；若为 SNAT 规则中最后一台云服务器，则联动删除 SNAT 规则。
由于标准协议限制，对于同一协议/目的 IP/目的端口，连接数上限 = 绑定的 EIP 数 * 55000，如需提升连接数，请新增绑定 EIP 或调整目的 IP/端口。

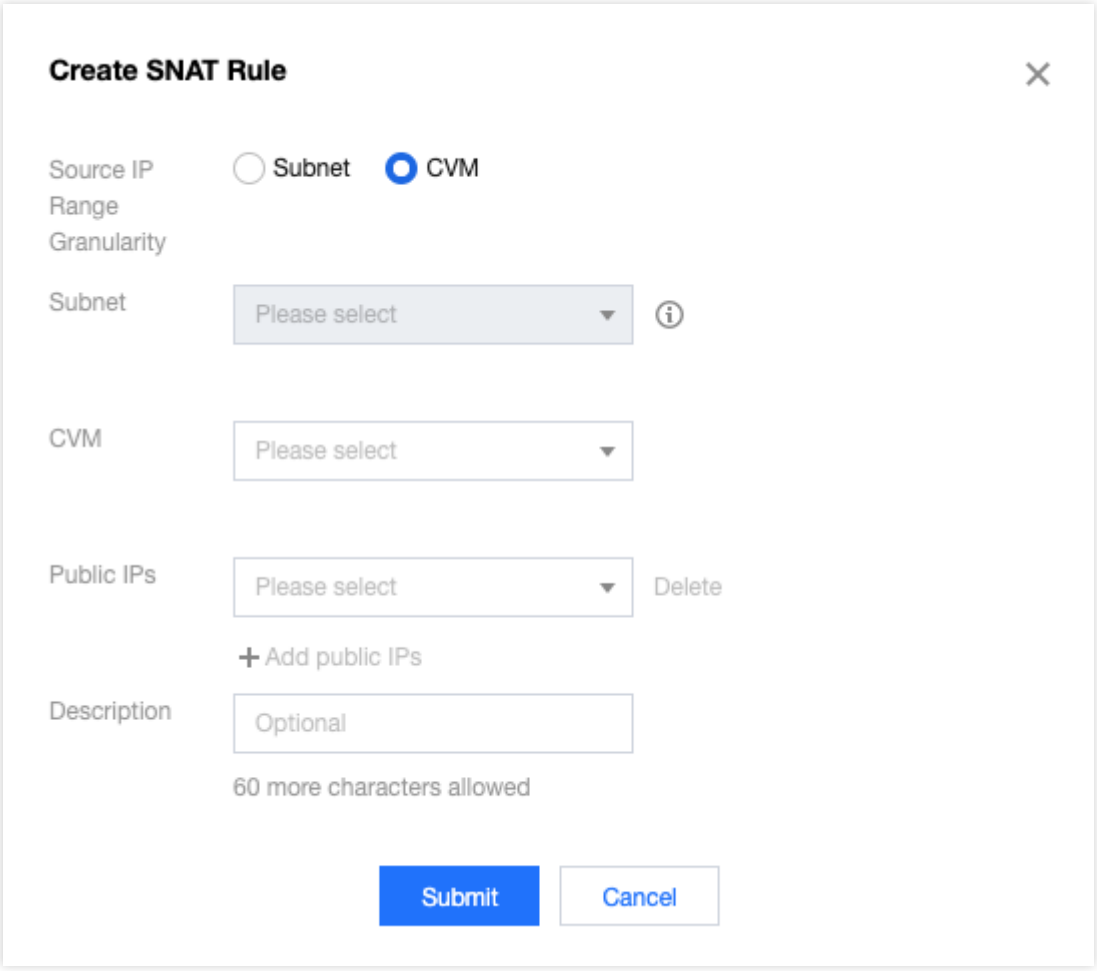
前提条件

创建 SNAT 规则前，请确保子网所在的路由表需指向对应的 NAT 网关，详细操作请参见 配置指向 NAT 网关的路由。

创建 SNAT 规则

1. 登录 NAT 网关控制台。
2. 在列表中单击网关 ID 进入详情页。
3. 选择**SNAT 规则**标签页，进入 SNAT 规则管理界面。
4. 单击**新建**，弹出**新建 SNAT 规则**对话框。
5. 设置 SNAT 规则。

源网段粒度：支持子网和云服务器粒度 。
子网：当选择子网时，子网所关联的路由表必须指向该 NAT 网关，该子网内的云服务器均按照 SNAT 规则访问外网。
云服务器：当选择云服务器时，云服务器所在子网所关联的路由表必须指向该 NAT 网关，只有选定的云服务器按照 SNAT 规则访问外网，没有配置 SNAT 规则的云服务器可以通过 NAT 上绑定的所有 EIP 访问公网。
所属子网：选择子网，或云服务器所在子网。
云服务器：仅当**源网段粒度**为**云服务器**时，需要指定云服务器，可添加多个云服务器。
公网 IP：指定访问公网的弹性公网IP。
描述：自定义描述信息，最多支持60个字符。



6. 完成 SNAT 规则的参数设置后，单击**提交**。

编辑 SNAT 规则

说明：
修改存量 SNAT 规则中的公网 IP，可能导致原有业务连接中断，重连后即可恢复，请谨慎操作。
1. 在 SNAT 规则标签页，单击 SNAT 规则条目右侧的**编辑**，进入编辑对话框。

2. 修改 SNAT 规则中的公网IP地址或描述，然后单击**提交**完成修改。
3. 单击 SNAT 规则中的描述信息旁的编辑图标，直接进行修改。

查询 SNAT 规则

1. 在 SNAT 规则标签页右上方的搜索框中，单击选择如下筛选条件，并在输入框中填写相应的参数值。
2. 单击搜索图标进行快速检索。
3. 单击子网/云服务器 ID，可跳转到相应资源详情界面。

删除 SNAT 规则

如果您不需要为云服务器访问外网指定 EIP，可删除 SNAT 规则。

单条删除

1.1 在 SNAT 规则标签页，单击 SNAT 规则条目右侧的**删除**。

1.2 单击**确认**，删除该条 SNAT 规则。

批量删除

1.1 在 SNAT 规则标签页，勾选多条 SNAT 规则，单击上方的**删除**。

1.2 在弹出的提示框中，单击**删除**，完成批量删除。

管理端口转发规则
新建端口转发规则

最近更新时间：2024-01-05 15:11:59

端口转发表是 NAT 网关上的一张配置表，用于配置 NAT 网关上的 DNAT 功能，可将 VPC 内云服务器的 **[内网 IP，协议，端口]** 映射成 **[外网 IP，协议，端口]**，使得云服务器上的资源可被外网访问。
下面将为您详细介绍如何新建端口转发规则。

说明：

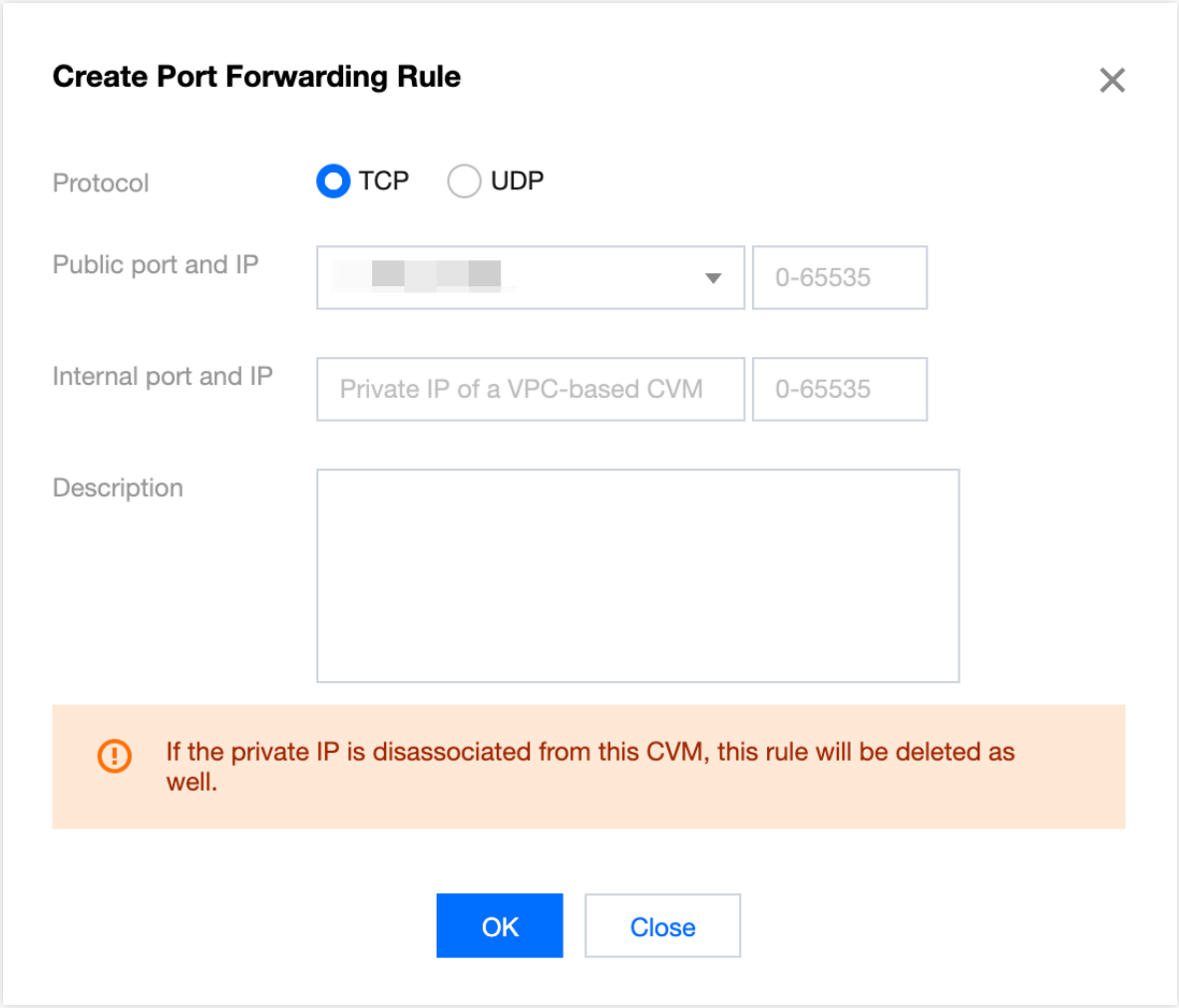
NAT 网关支持将同一个 EIP 同时用于配置端口转发规则和 SNAT 规则，SNAT 规则的详细信息请参考 管理 SNAT 规则。

1. 登录 NAT 网关控制台。
2. 在列表中单击需要修改的 NAT 网关 ID 进入详情页，单击选项卡中的**端口转发**。

3. 单击**新建**，选择协议、外部端口 IP 及内部端口 IP 后，单击**确定**即可。

注意：

内部 IP 仅支持该 VPC 内的云服务器内网 IP。


Create Port Forwarding Rule
Protocol
TCP
UDP
Public port and IP
0-65535
Internal port and IP
Private IP of a VPC-based CVM
0-65535
Description
If the private IP is disassociated from this CVM, this rule will be deleted as well.
OK
Close

查询端口转发规则

最近更新时间：2024-01-05 15:11:59

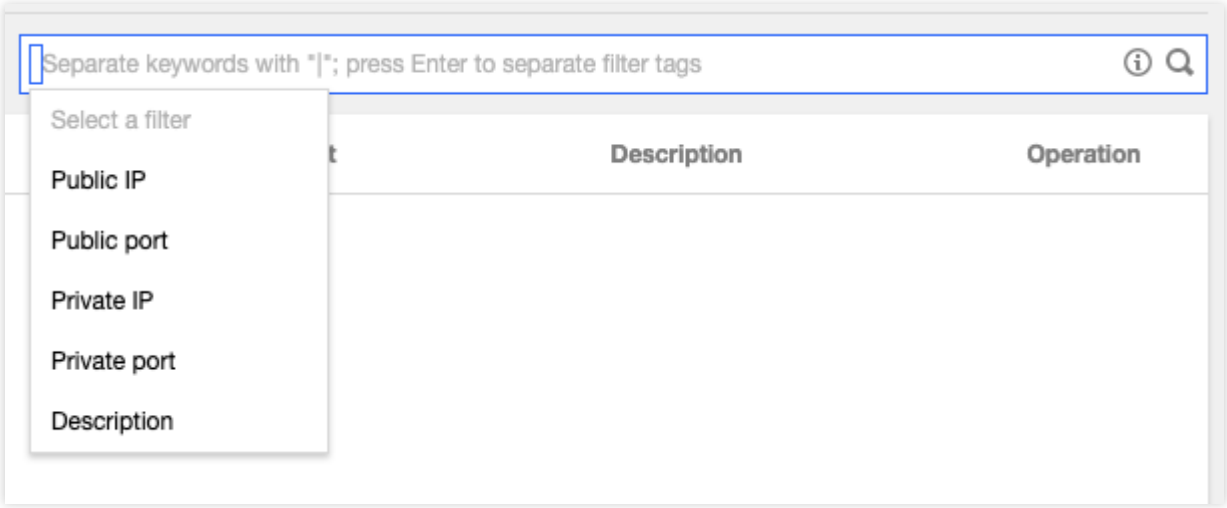
下面将为您详细介绍如何查询端口转发规则。

1. 登录 NAT 网关控制台。
2. 在列表中单击需要查询的 NAT 网关 ID 进入详情页，单击选项卡中的**端口转发**。

3. 在搜索框内，选择资源属性值或输入关键字后，即可查询相关端口转发规则。

说明：

请检查是否已经在实例所在子网关联的路由表内添加了 NAT 网关路由策略。



公网 NAT 使用限制

最近更新时间：2024-01-05 15:11:59

本文介绍 NAT 网关的使用规则和使用限制。

说明：

NAT 网关支持 TCP、UDP 和 ICMP 协议，而 GRE 隧道和 IPSec 使用的 ESP、AH 无法使用 NAT 网关，且暂不支持 ALG 相关技术。这是由 NAT 网关本身的特性决定的，与服务提供商无关。当前互联网大部分应用都是 TCP 应用，TCP 和 UDP 应用总和约占互联网应用类型的99%。

使用规则

在使用 NAT 网关时，您需要注意以下几点：

用户删除 NAT 网关会解除其弹性公网 IP 地址的关联，但不会从用户帐号释放该弹性 IP 地址。

用户不能为 NAT 网关关联安全组，但可以为私有子网中的实例绑定安全组，以控制进出这些实例的流量。

用户无法直接使用网络 ACL 控制进出 NAT 网关的流量，但可以使用网络 ACL 控制进出 NAT 网关所关联子网的流量。

用户无法通过 VPC 对等连接、VPN 连接将流量路由到 NAT 网关，因为此类连接另一端的资源不能使用 NAT 网关。例如，VPC 1 发往 Internet 的流量都可通过 NAT 网关实现， VPC 1 和 VPC 2 建立了对等连接，VPC 2 中所有的资源可访问 VPC 1 中的所有资源，但 VPC 2 中的所有资源不可以通过 NAT 网关访问 Internet。

SNAT 规则限制

当 NAT 网关解关联 EIP 时，若该 EIP 为 SNAT 规则的唯一 EIP，则同时删除此条 SNAT 规则；若该 EIP 为此 SNAT 规则的非唯一 EIP，则 SNAT 规则中删除此 EIP。

SNAT 规则中使用的子网不存在时，联动删除该 SNAT 规则。

SNAT 规则中使用的云服务器不存在时，联动从 SNAT 规则中删除该云服务器；若为 SNAT 规则中最后一台云服务器，则联动删除 SNAT 规则。

由于标准协议限制，对于同一协议/目的 IP/目的端口，连接数上限 = 绑定的 EIP 数 * 55000，如需提升连接数，请新增绑定 EIP 或调整目的 IP/端口，目的 IP/端口。

NAT 网关相关配额限制

NAT 网关支持的资源限制如下表所示，您还可以查看 VPC 其它产品的配额限制。

资源	限制

每个 VPC 支持的 NAT 网关数	3个
每个 NAT 网关支持弹性 IP 个数	10
每个 NAT 网关最多支持转发能力	5Gbps
每个 NAT 网关的最大端口转发条数	200
每个 NAT 网关的 SNAT 规则条目数	200条

NAT 网关流日志

最近更新时间：2024-01-05 15:11:58

NAT 网关提供流日志采集功能，通过对 NAT 网关流量的采集分析，并形成日志记录和图表分析，以便您能及时了解跨域通信情况，根据日志快速定位问题并解决，从而提升业务可用性及运维效率。

说明：

目前网络流日志处于内测中，如有需要，请 提交工单。

流日志本身不会产生费用，数据存储在日志服务中，将按日志服务的 标准收费。

流日志数据存储在日志服务 CLS 中，请确保已完成 授权流日志访问 CLS 权限，否则无法在 CLS 上查询到日志数据。

操作步骤

1. 登录 私有网络控制台，在左侧导航栏中单击**流日志** > **日志列表**。
2. 在“流日志”页面左上角选择地域，然后单击**+新建**。
3. 在“新建流日志”对话框中配置如下参数。

字段	含义
名称	该流日志的名称。
采集范围	目前支持多个采集范围，此处选择“NAT 网关”。
NAT 网关	NAT 网关的信息。
采集类型	指定流日志应捕获被安全组或 ACL 已拒绝流量、已接受流量、或所有流量。
日志集	指定流日志在日志服务内的存储集合。如已有日志集，请直接选择；如无，可保持“系统默认创建”，由系统帮您创建，或单击新建前往日志服务控制台自行创建。
日志主题	指定日志存储的最小维度，用于区别不同类型日志，例如 Accept 日志等。 如已有日志主题，请直接选择；如无，可保持“系统默认创建”，由系统帮您创建，或前往日志服务控制台自行创建。 **说明：** 日志集和日志主题及索引的配置请参见 创建日志集和日志主题。
标签键	单击**高级选项**，您可以新建（直接输入）或选择已有标签键，用于流日志查找和管理。
标签值	单击**高级选项**，您可以新建（直接输入）或选择已有标签值，也可以为空值。

4. 单击**确定**，即可完成流日志的创建。

说明：

首次创建流日志需要约6分钟后（1分钟捕获窗口，5分钟数据推送时间），方可在日志服务中查看流日志。

5. 等待约6分钟后，单击**存储位置**，或**查看**进入日志服务的“检索分析”界面，选择要查看日志的地域，时间段等，单击**检索分析**，查看日志记录。

说明：

字段解释请参见 流日志记录，日志分析请参见 快速分析。

绑定高防包

最近更新时间：2024-01-05 15:11:59

您可为 NAT 网关绑定 DDoS 高防包以抵御 DDoS 攻击。

1. 购买 DDoS 高防包。
2. 为 NAT 网关配置 DDoS 高防包，详细操作请参见 DDoS 高防包快速入门。

告警与监控
设置告警

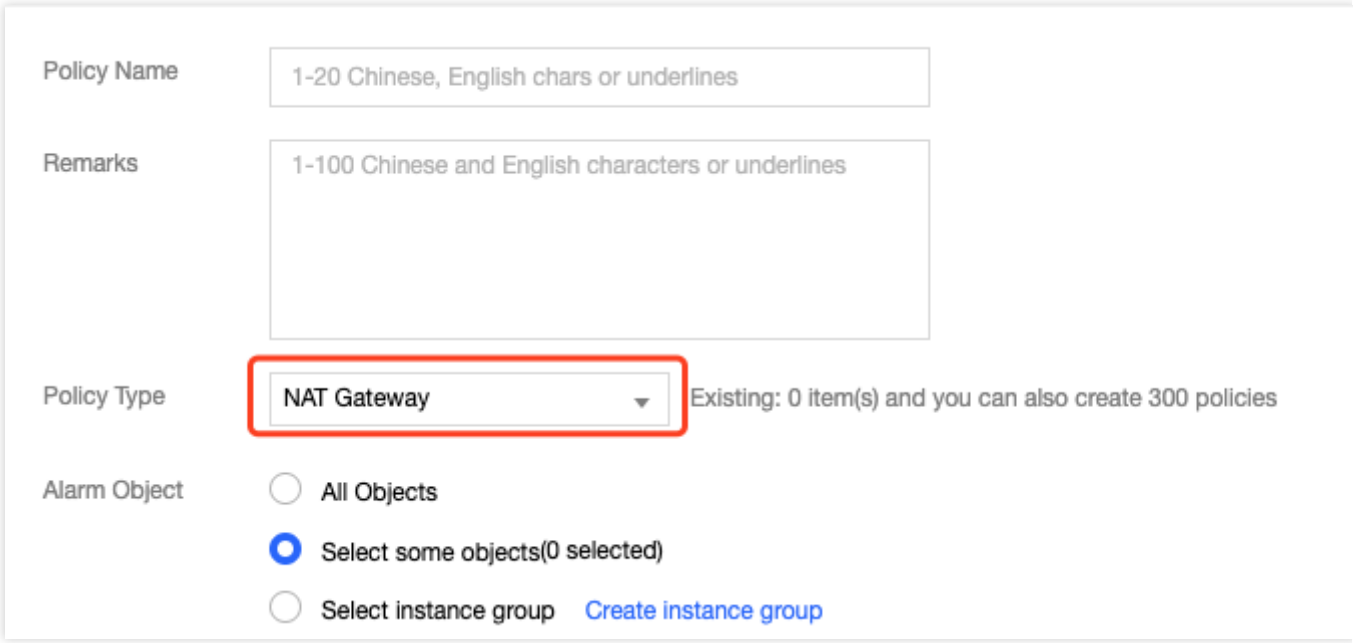
最近更新时间：2024-01-05 15:11:59

您可以为 NAT 网关设置告警来监控 NAT 网关的状态。

1. 登录 云监控控制台。

2. 在左侧目录选择**告警配置** > **告警策略**，进入告警策略配置页面，单击**新增**。

3. 填写告警策略名称和备注，策略类型选择**私有网络** > **NAT 网关**，选择告警对象、策略触发条件和告警渠道，如有需要可填写公网可访问到的 URL 作为回调接口地址，云监控将及时把告警信息推送到该地址。



4. 单击**完成**，即可在告警策略列表中查看已设置的告警策略。

说明：

告警策略创建后，需要解绑所有资源才能删除。

5. 告警条件被触发后，您将通过已选择的告警渠道接收到告警通知（短信 / 邮件 / 站内信等），也可以单击左侧目录【告警历史】查看告警信息。更多告警相关信息，请参见 新建告警策略。

说明：

由于带宽最细统计粒度为10秒（10秒内总流量/10秒），因此带宽毛刺导致的丢包不一定会体现在带宽视图中。

查看监控信息

最近更新时间：2024-01-05 15:11:59

创建 NAT 网关后，您可以通过控制台查看监控信息并导出数据。

1. 登录 NAT 网关控制台。
2. 在 NAT 网关列表中，单击需要查看的网关 ID 进入详情页。
3. 单击**监控**选项卡查看监控信息。

单击

支持**数据导出**或**图片导出**，可将数据保存到本地。

单击

可全屏展示图表。

单击

可配置告警。

4. （可选）您也可以在 NAT 网关列表中，单击需要查看的 NAT 网关条目中的监控按钮，即可查看监控信息。

删除 NAT 网关

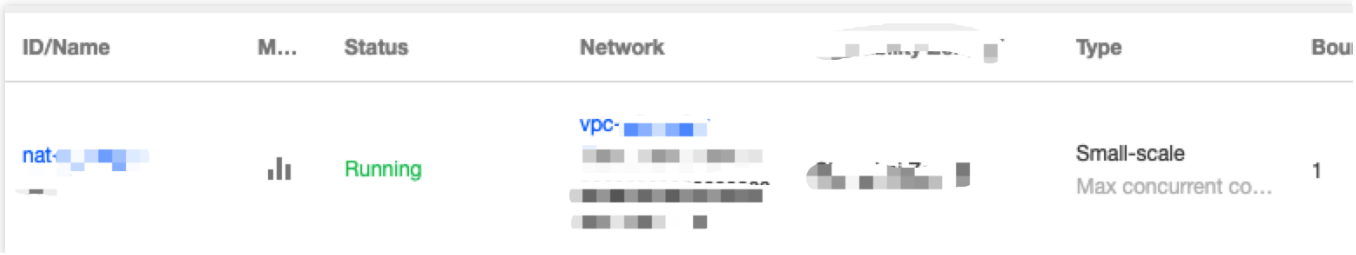
最近更新时间：2024-01-05 15:11:59

注意：

删除时会将含有此 NAT 网关的路由表相关路由策略一并删除，Internet 转发请求将立即中断，请提前做好网络中断准备。

在确定无需使用 NAT 网关后，您可以随时将其删除。

1. 登录 NAT 网关控制台。
2. 在列表中找到需要删除的 NAT 网关，单击操作栏下的**删除**并确认操作即可。



调整 NAT 网关和 EIP 的优先级

最近更新时间：2024-01-05 15:11:59

NAT 网关/EIP 优先级说明

当一个子网关联了 NAT 网关，且子网内云服务器有公网 IP（或弹性 IP）时，会默认通过 NAT网关访问 Internet（因为最精确路由的优先级高于公网 IP），但您可以设置路由策略，实现通过云服务器公网 IP 访问 Internet。

操作步骤

1. 查看该云服务器所在子网关联的路由表。确保有指向 NAT 网关的路由策略，以保证该子网下，无公网 IP 的云服务器仍可以通过 NAT 网关访问 Internet 。
2. 新增下一跳类型为“云服务器的公网 IP”的路由策略，并填入目的端。
目的端：填写业务需要访问的具体公网网段或默认路由（0.0.0.0/0，默认路由表示：目的端不在路由表中，所有数据包都会使用该默认路由）。
下一跳类型：云服务器的公网 IP。

说明：

此路由策略与原来指向 NAT 网关、云服务器、公网网关的路由规则配置相同目的端时，均会优先匹配该路由。
此路由策略会影响该路由表关联的所有子网（请您确认操作带来的影响），即这些子网内有公网 IP（或弹性 IP）的云服务器访问 Internet，将不再通过 NAT 网关，而是其公网 IP。
该路由表关联的子网内，无公网 IP 的云服务器仍可以通过 NAT 网关访问 Internet，不会受到影响。