网络流日志

产品简介

产品文档

腾讯云

文档目录

产品简介

产品概述

最近更新时间：2024-01-10 16:10:45

网络流日志（Flow logs）为您提供全时、全流、非侵入的流量采集服务，可将采集的网络流量进行实时的存储、分析，适用于故障排查、合规审计、架构优化、安全检测等场景，让您的云上网络更加稳定、安全和智能。

您可以创建指定采集范围（例如弹性网卡、NAT 网关、云联网跨地域流量）的网络流日志，来采集该范围内传入/传出的流量。创建流日志后，您可以在 日志服务（CLS） 中查看和检索数据，也可以在高级分析仪表盘中直观查看日志数据。

说明：

目前 NAT 网关、云联网跨地域流量流日志处于内测中，如有需要，请提交 工单申请。

产品优势

最近更新时间：2024-01-10 16:10:45

无性能损耗

非侵入的采集，从根源上解决传统采集方式大量消耗云服务器带宽及 CPU 的痛点。

安全

旁路采集使您无需在云服务器内安装任何插件，解决您的安全顾虑，故障发生时也可明确无采集方的责任。

全时全流

强大的包处理能力，可采集全网的弹性网卡流量，准确展现业务网络状况，让您对云网络质量了如指掌。

实时性强

实时的海量网络流数据采集，帮助企业迅速实现业务分析、趋势判断与决策响应。

简单易管理

秒级开通、简单易管理，帮助您提升运维效率，使您的企业更专注于核心业务创新，提升企业竞争力。

可视化分析

通过仪表盘可直观展示、分析流日志数据，简单易用，运维效率更高。

产品功能

最近更新时间：2024-01-10 16:10:45

流日志具有日志采集、查询、数据管理、数据记录与分析等功能，帮助您降低运维门槛，轻松定位业务问题。

流日志采集

创建流日志后，系统将自动采集指定范围（例如弹性网卡、NAT 网关、云联网跨地域流量）的日志流，并将日志数据投递并存储于 日志服务 CLS。在 CLS 的主题中，每个弹性网卡有唯一的日志流，其中包含流日志记录。

说明：

NAT 网关和云联网跨地域流量流日志目前处于内测中，如有需要，请提交 工单申请。

流日志查询

流日志在 日志服务 CLS 平台进行查询及消费。日志服务 CLS 支持亿级日志数据检索，您可以进行全文检索、多关键词检索、跨主题查询等操作，秒级返回查询结果。

流日志存储

流日志与 日志服务 CLS 深度结合，实现对日志数据的存储与管理。

创建仪表盘多维度展示日志数据

在流日志专用日志集“flowlog_logset”下，可针对弹性网卡类型流日志创建仪表盘，最终通过仪表盘来可视化观测、分析流日志数据。一个日志主题可创建一个仪表盘。

仪表盘数据展示如下图所示，具体配置请参见 高级分析。

流日志记录

流日志将记录特定捕获窗口中，按一定规则过滤的网络流。

云联网跨地域流量的网络流日志记录

其他类型的网络流日志记录

流日志将记录特定捕获窗口中，按“五元组 + 流量源地域 + 流量目的地域”规则过滤的网络流，即只有在捕获窗口中符合规则的网络流日志，才能记录为云联网跨地域流量的网络流日志记录。

五元组 + 流量源地域 + 流量目的地域

五元组即源 IP 地址、源端口、目的 IP 地址、目的端口和传输层协议这五个量组成的一个集合。

流量源地域指云联网跨地域流量发出的地域。

流量目的地域指云联网跨地域流量到达的地域。

捕获窗口

即一段持续时间，在这段时间内流日志服务会聚合数据，然后再发布流日志记录。捕获窗口大约为1分钟，推送时间约为5分钟。流日志记录是以空格分隔的字符串，采用以下格式：

```
srcaddr dstregionid dstport start dstaddr version packets ccnid protocol
srcregionid bytes action region-id srcport end log-status
```

字段	数据类型	说明
srcaddr	text	源 IP。
dstregionid	text	流量目的地域。
dstport	long	流量的目标端口。该字段仅对 UDP/TCP 协议生效，当流量为其他协议时，该字段显示为“-”。
start	long	当前捕获窗口收到第一个报文的时间戳，如果在捕获窗口内没有报文，则显示为该捕获窗口的起始时间，采用 Unix 秒的格式。
dstaddr	text	目标 IP。
version	text	流日志版本。
packets	long	捕获窗口中传输的数据包的数量。当“log-status”为“NODATA”时，该字段显示为“-”。
ccn-id	text	云联网唯一标识，如需确定云联网的信息请 联系我们。
protocol	long	流量的 IANA 协议编号。有关更多信息，请转到分配的 Internet 协议 编号。
srcregionid	text	流量源地域。
bytes	long	捕获窗口中传输的字节数。当“log-status”为“NODATA”时，该字段显示为“-”。
action	text	与流量关联的操作： ACCEPT：通过云联网正常转发的跨地域流量。 REJECT：因限速被阻止转发的跨地域流量。
region-id	text	记录日志的地域。

srcport	text	流量的源端口。该字段仅对 UDP/TCP 协议生效，当流量为其他协议时，该字段显示为“-”。
end	long	当前捕获窗口收到最后一个报文的时间戳，如果在捕获窗口内没有报文，则显示为该捕获窗口的结束时间，采用 Unix 秒的格式。
log-status	text	流日志的日志记录状态： OK：表示数据正常记录到指定目标。 NODATA：表示捕获窗口中没有传入或传出网络流量，此时“packets”和“bytes”字段会显示为“-1”。

流日志将记录特定捕获窗口中，按五元组规则过滤的网络流。

五元组

即源 IP 地址，源端口，目的 IP 地址，目的端口和传输层协议这五个量组成的一个集合。

捕获窗口

即一段持续时间，在这段时间内流日志服务会聚合数据，然后再发布流日志记录。捕获窗口大约为5分钟，推送时间约为5分钟。流日志记录是以空格分隔的字符串，采用以下格式：

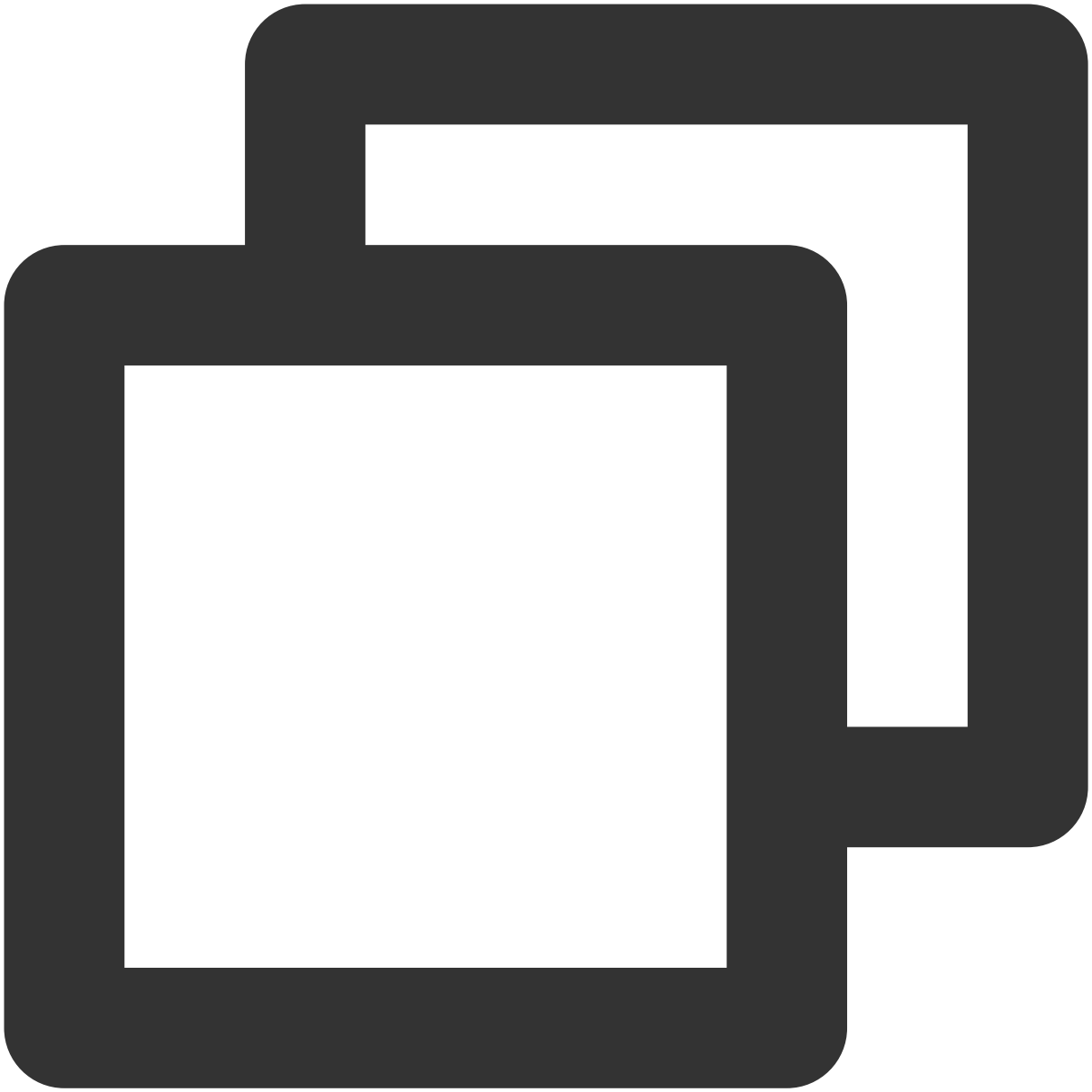
`version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status` 。

字段	说明
version	流日志版本。
account-id	流日志的账户 AppID。
interface-id	弹性网卡 ID。
srcaddr	源 IP。
dstaddr	目标 IP。
srcport	流量的源端口。当流量为 ICMP 协议时，该字段表示 ICMP 的 id。
dstport	流量的目标端口。当流量为 ICMP 协议时，该字段表示 ICMP 的 type（高8bit）+code（低8bit）组合。
protocol	流量的 IANA 协议编号。有关更多信息，请转到分配的 Internet 协议 编号。
packets	捕获窗口中传输的数据包的数量。
bytes	捕获窗口中传输的字节数。
start	捕获窗口启动的时间，采用 Unix 秒的格式。

end	捕获窗口结束的时间，采用 Unix 秒的格式。
action	与流量关联的操作： ACCEPT：安全组或网络 ACL 允许记录的流量。 REJECT：安全组或网络 ACL 未允许记录的流量。
log-status	流日志的日志记录状态： OK：表示数据正常记录到指定目标。 NODATA：表示捕获窗口中没有传入或传出网络流量，此时“packets”和“bytes”字段会显示为“-1”。 SKIPDATA：表示捕获窗口中跳过了一些流日志记录。可能是内部容量限制或内部错误引起的。

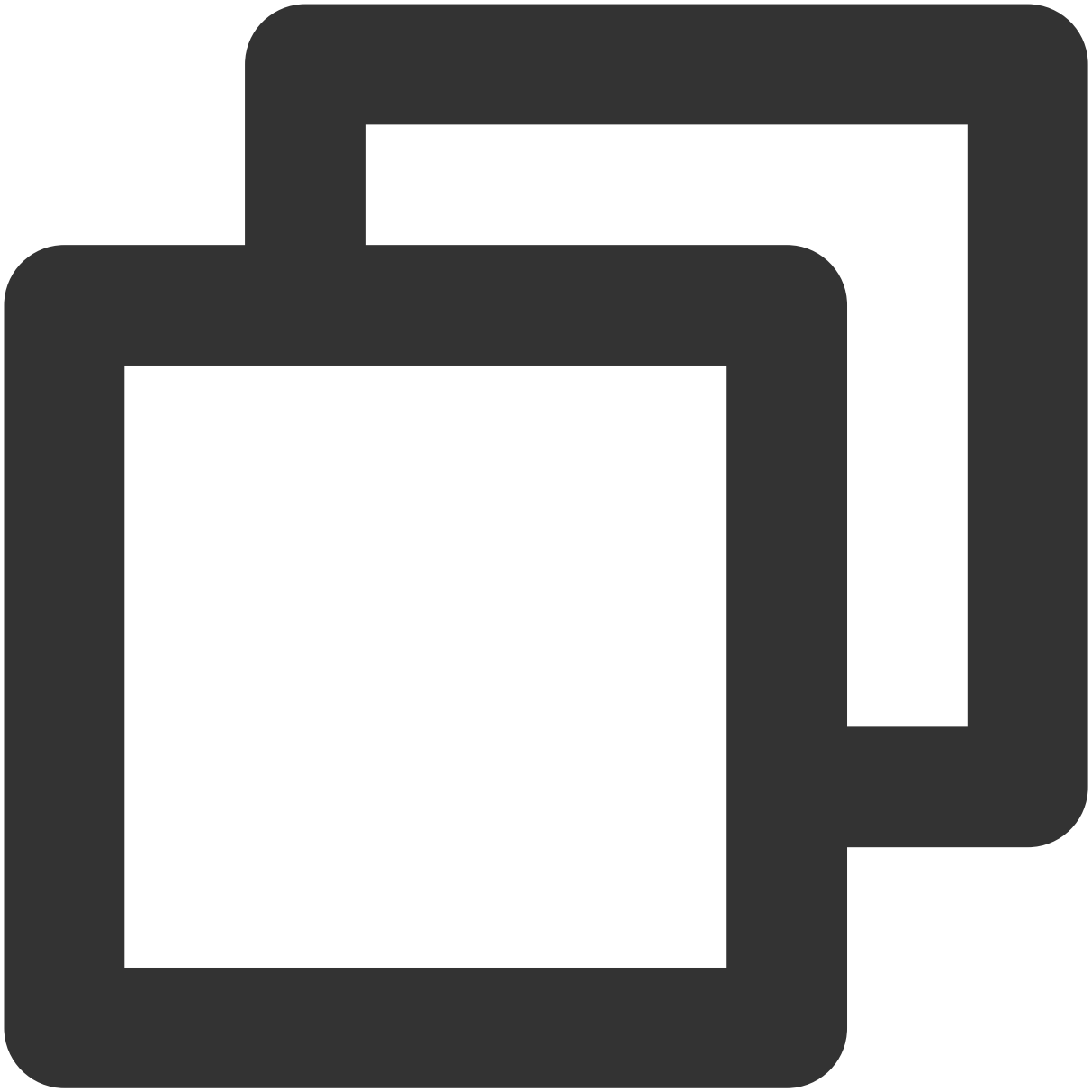
示例

若允许接受账户 1251762227 中的弹性网卡 eni-lq6mkcis 的 SSH 流量（目标端口 22，TCP 协议），流日志记录如下：



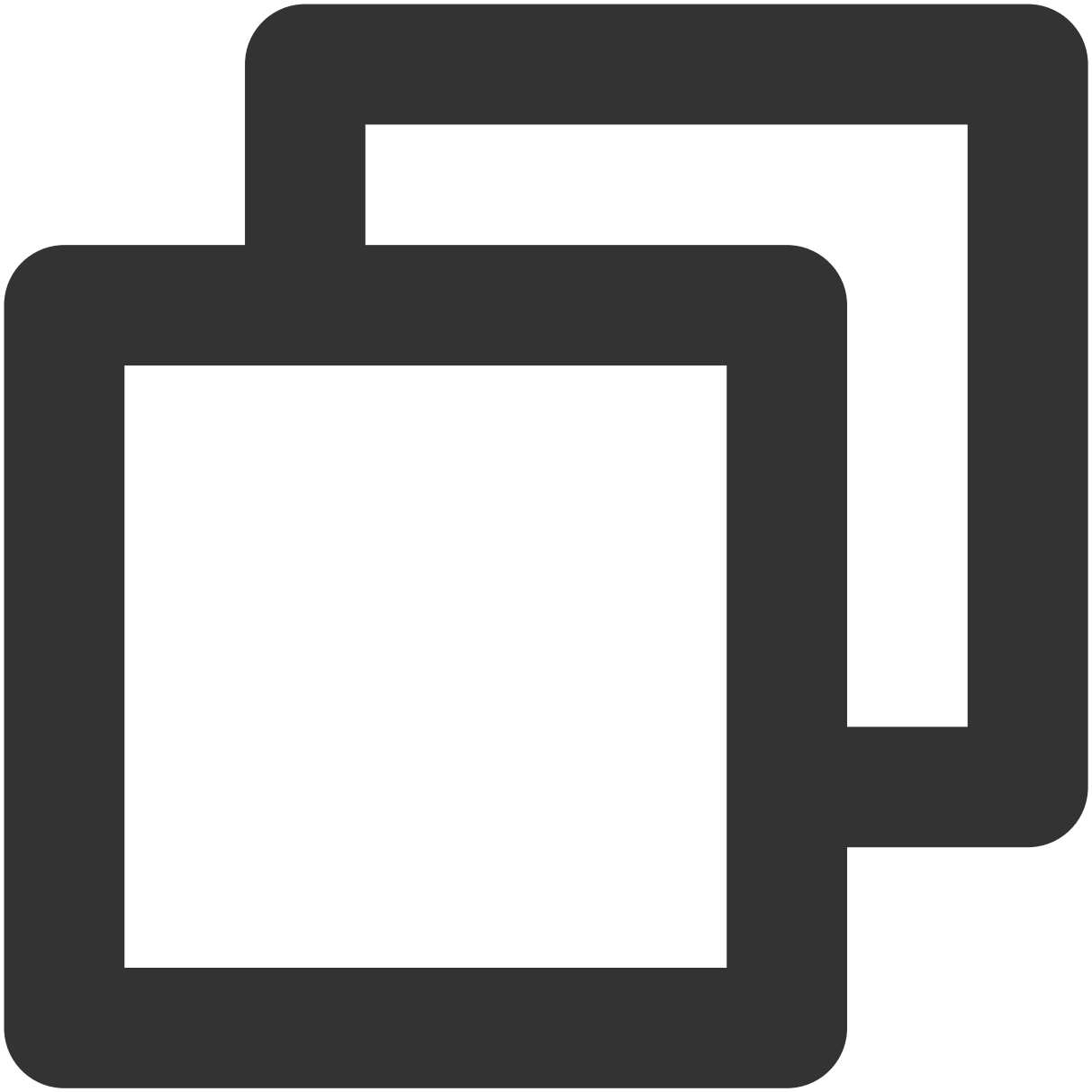
```
2 1251762227 eni-lq6mkcis 172.31.16.139 172.31.16.21 20641 22 6 20 4249 1418530010
```

若拒绝账户1251762227中的弹性网卡 eni-lq6mkcis 的 RDP 流量（目标端口3389，TCP 协议），流日志记录如下：



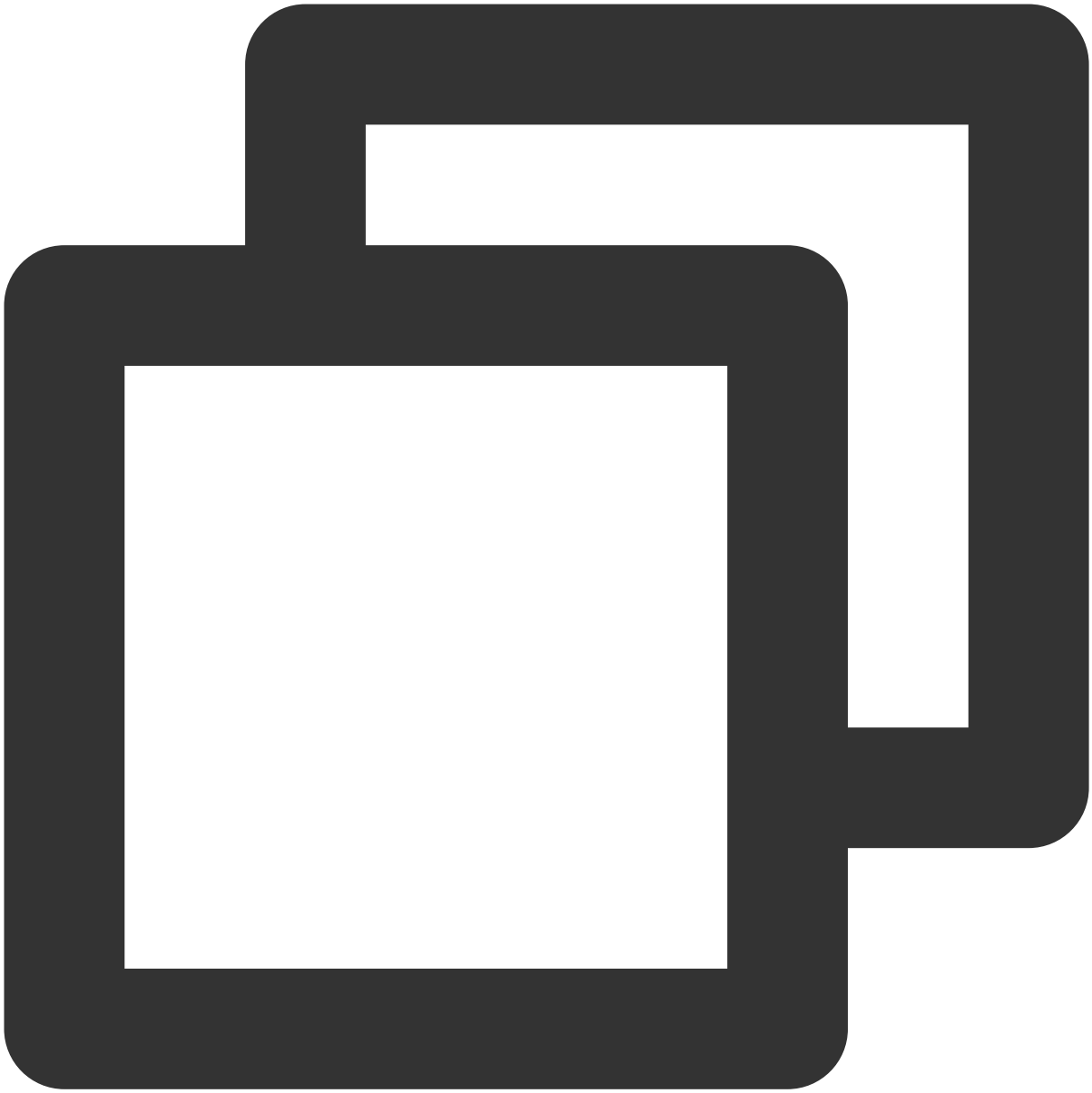
```
2 1251762227 eni-lq6mkcis 172.31.9.69 172.31.9.12 49761 3389 6 20 4249 1418530010 1
```

若在捕获窗口中未记录数据，流日志记录如下：



```
V1 1251762227 eni-lq6mkcis - - - - - - - 1431280876 1431280934 - NODATA
```

若在捕获窗口中跳过了记录，流日志记录如下：



```
V1 1251762227 eni-lq6mkcis - - - - - - - 1431280876 1431280934 - SKIPDATA
```

安全组和网络 ACL 规则的流日志记录

安全组为有状态，因此允许响应所有的流量。

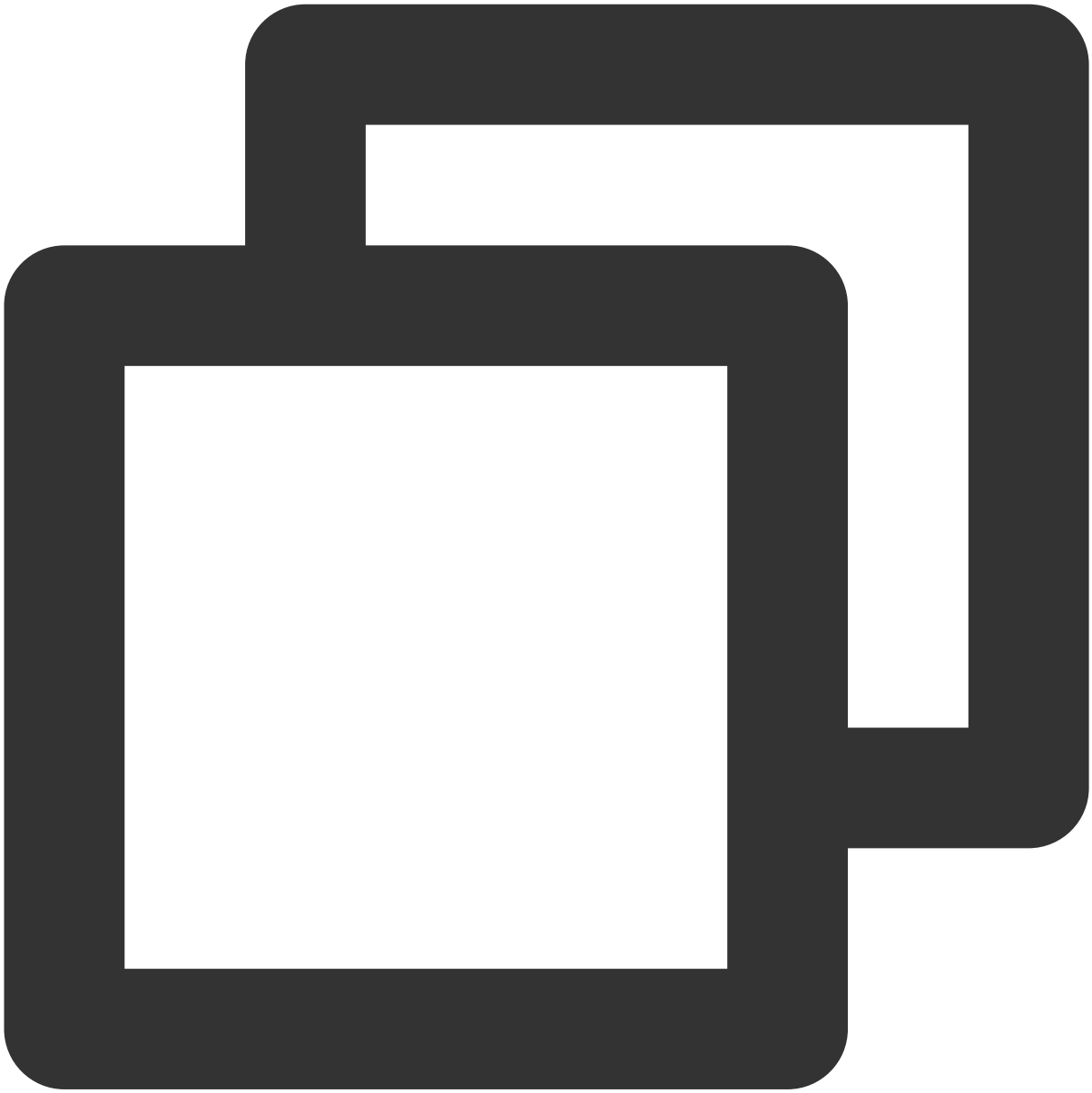
网络 ACL 为无状态，因此对流量的响应需要遵守网络 ACL 规则。

例如，您从家中的计算机（IP 地址为 `203.0.113.12` ）对您的实例（网络接口的私有 IP 地址为 `172.31.16.139` ）使用 ping 命令。您的安全组入站规则允许 ICMP 流量，出站规则不允许 ICMP 流量，但是，由于安全组是有状态的，因此允许从您的实例响应 ping。

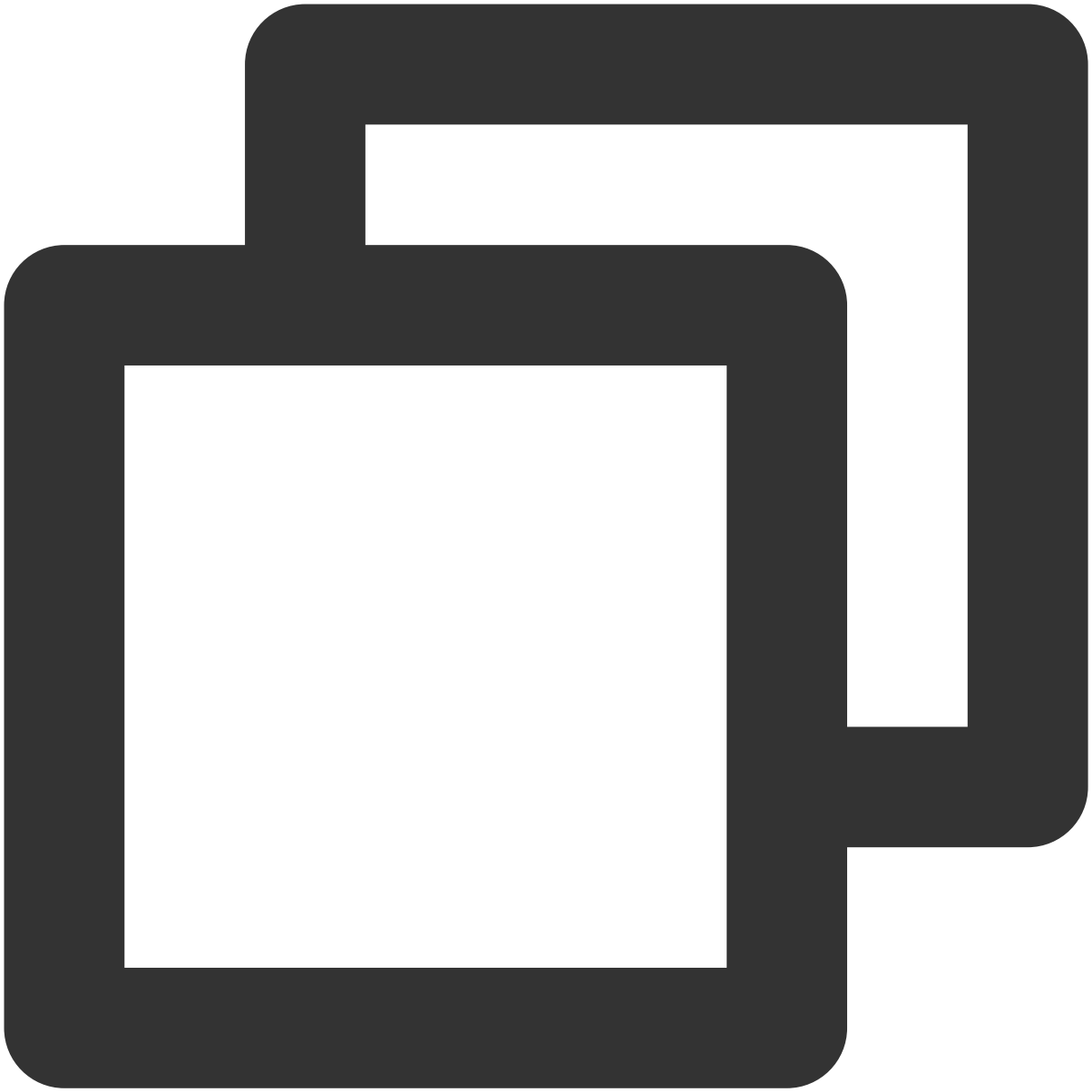
您的网络 ACL 允许入站 ICMP 流量，但不允许出站 ICMP 流量。由于网络 ACL 是无状态的，响应 ping 将被丢弃，不会传输到您家中的计算机。在流日志中，它显示为2个流日志记录：

网络 ACL 和安全组都允许（因此可到达您的实例）的发起 ping 的 ACCEPT 记录。

网络 ACL 拒绝的响应 ping 的 REJECT 记录。



```
V1 1251762227 eni-lq6mkcis 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 143291
```



```
V1 1251762227 eni-lq6mkcis 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 143291
```

如果您的网络 ACL 允许出站 ICMP 流量，流日志会显示两个 ACCEPT 记录（一个针对发起 ping，一个针对响应 ping）。如果您的安全组拒绝入站 ICMP 流量，流日志会显示一个 REJECT 记录，因为流量未到达您的实例。

应用场景

最近更新时间：2024-01-10 16:10:45

快速定位网络故障

网络质量是业务稳定的基石，通过流日志可保存故障现场，助力您快速定位网络故障，进行网络回溯取证，减少网络停用时间。具体如下：

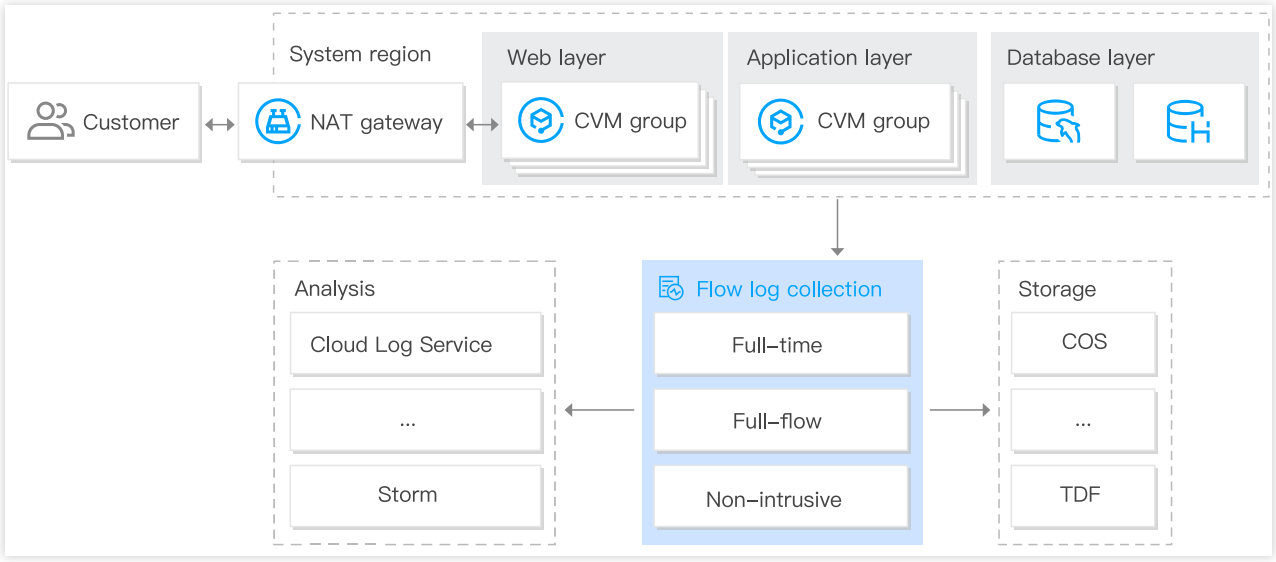
快速定位问题根源的云服务器，例如广播风暴、带宽过度使用的云服务器。

快速定位云服务器不可访问是否为安全组或 ACL 设置不合理。

配置建议：

创建流日志采集网卡流量。

网络日志投递至日志服务进行查询、分析或存储。



合理优化网络架构

流日志可采集全网、全时、全流的弹性网卡流量，通过大数据分析及可视化，助力您提升数据驱动的网络运维能力，合理优化网络架构。具体如下：

分析历史网络数据，构建业务网络基准。

及时发现性能瓶颈，合理扩容或流量降级。

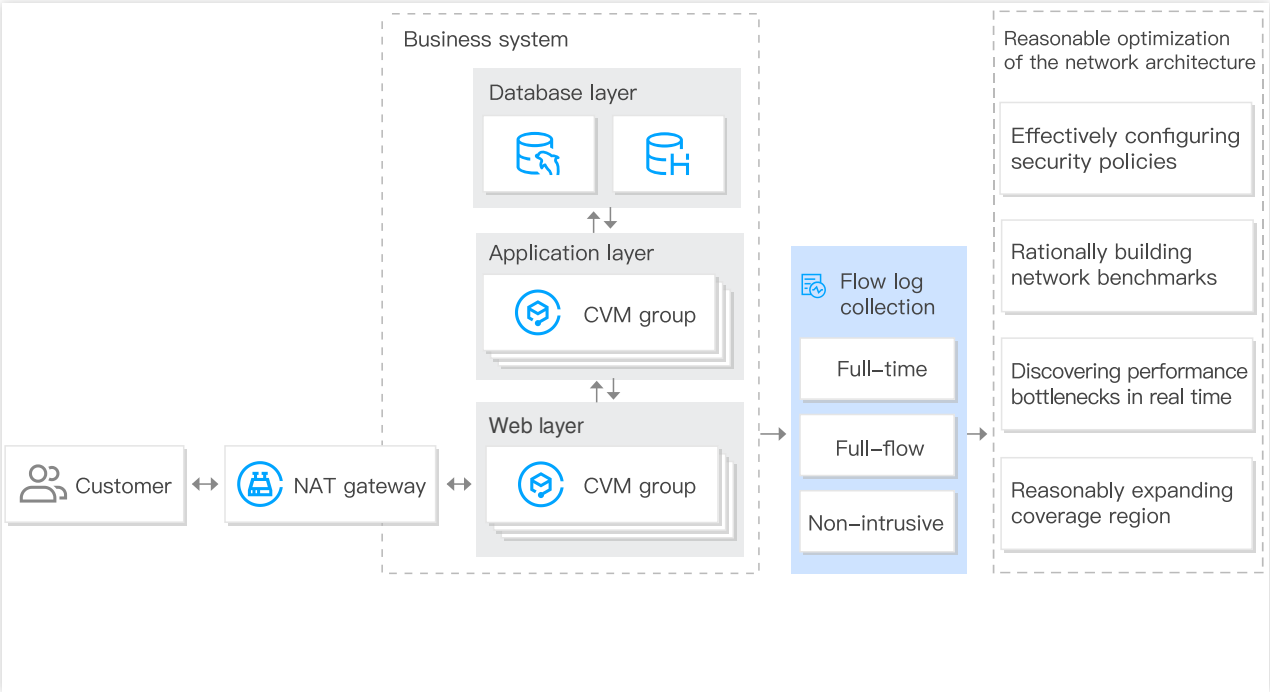
分析访问用户地域，合理拓展覆盖域。

分析网络流量，优化网络安全策略。

配置建议：

创建流日志采集网卡流量。

网络日志投递至日志服务进行分析。



迅速发现网络安全威胁

传统流量检查点的增加，会引起云服务器性能下降，流日志采用全时、全流、非侵入的采集方式，助力您在不影响云服务器性能情况下，及时发现网络安全威胁，提升系统的安全性。具体如下：

试图连接大范围 IP。

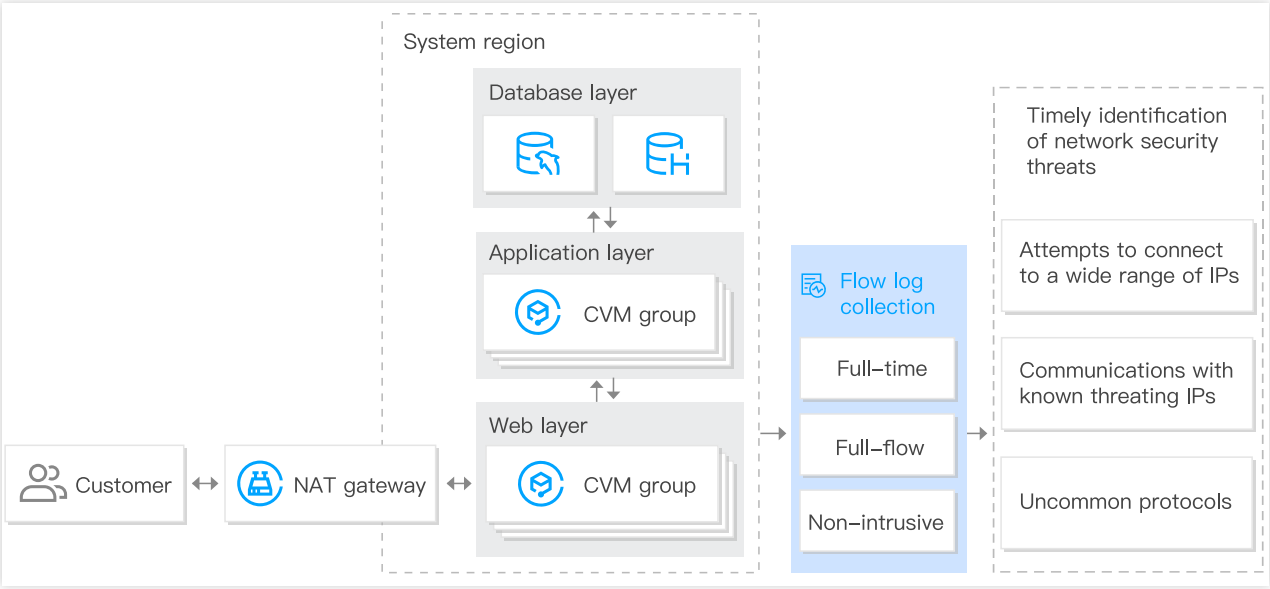
与已知威胁 IP 通信。

识别出不常用协议。

配置建议：

创建流日志采集网络流量。

网络日志投递至日志服务进行查询与分析。


System region
Database layer
Application layer
CVM group
Web layer
CVM group
Customer
NAT gateway
Flow log collection
Full-time
Full-flow
Non-intrusive
Timely identification of network security threats
Attempts to connect to a wide range of IPs
Communications with known threating IPs
Uncommon protocols

使用限制

最近更新时间：2024-01-10 16:10:45

注意事项

网络流日志仅支持采集 VPC 范围内弹性网卡、NAT 网关、云联网跨地域流量的流日志，不支持采集基础网络范围内的流日志。

说明：

目前 NAT 网关、云联网跨地域流量流日志处于内测中，如有需要，请提交 工单申请。

流日志功能支持所有地域，但 CLS 侧存在地域限制，导致部分地域数据可能无法投递到 CLS，具体请参见 CLS 可用地域。

创建流日志后，您不能更改其配置（如修改流日志投递的日志服务）。

流日志不支持采集的 IP 流量类型：

Windows 实例为 Windows 许可证激活而生成的流量。

DHCP 流量。

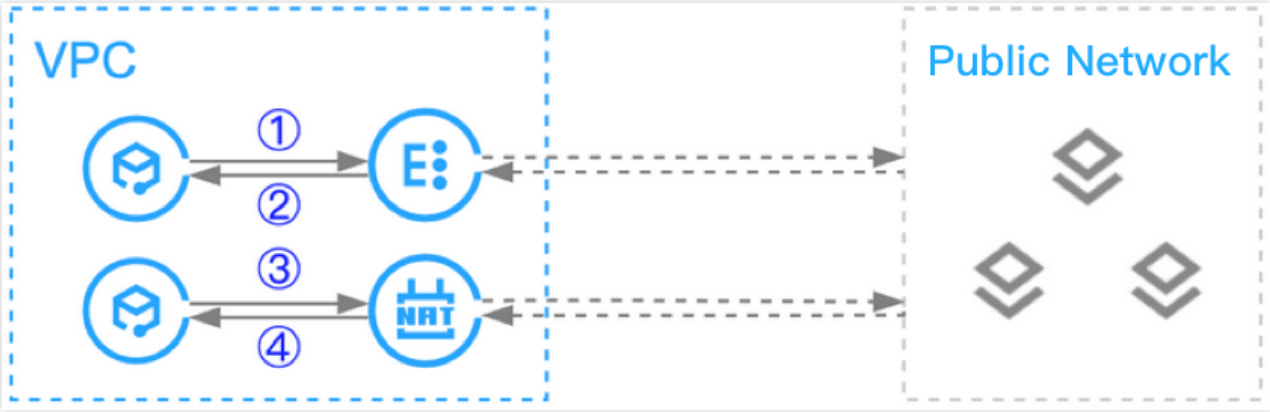
1个弹性网卡仅能创建1个流日志。

网络流日志采集云服务器上弹性网卡的流量时，出方向采集限速前的流量，入方向是限速后的流量。

例如，若为云服务器的弹性网卡创建网络流日志：

当云服务器通过负载均衡访问公网时，则出方向采集箭头1的流量，入方向采集箭头2的流量。

当云服务器通过 NAT 网关访问公网时，则出方向采集箭头3的流量，入方向采集箭头4的流量。



支持仪表盘功能的流日志类型

目前仅弹性网卡类型、且日志集和日志主题携带“Flowlog”标识的流日志，支持创建或查看高级分析仪表盘。

说明：

在 主题配置 中可创建携带“Flowlog”标识的日志集“flowlog_logset”和日志主题。

机型限制

支持流日志进行采集的 云服务器实例规格 包括：M6ce、M6p、SA3se、S4m、DA3、ITA3、I6t、I6、SA3、S5se、SA2、SK1、S4、S5、SN3ne、S3ne、S2ne、SA2a、S3ne、SW3a、SW3b、SW3ne、ITA3、IT5c、IT5、IT5c、IT3、I3、D3、DA2、D2、M6、MA2、M4、C6、IT3a、IT3b、IT3c、C4ne、CN3ne、C3ne、GI1、PNV4、GNV4v、GNV4、GT4、GI3X、GN7、GN7vw

如下机型不再支持新建流日志进行采集，存量流日志也将于 2022年7月25日 起不再进行数据上报：

标准型：S3、SA1、S2、S1

内存型：M3、M2、M1

计算型：C4、CN3、C3、C2

批量计算型：BC1、BS1

高性能计算集群：HCCIC5、HCCG5v

相关产品

最近更新时间：2024-01-10 16:10:45

网络流日志的相关产品信息，请参见下表：

产品名称	与网络流日志的关系
云服务器	网络流日志可快速定位问题根源的云服务器
CLS 日志服务	网络流日志可投递至 CLS 日志服务中，满足日志审计需求
安全组	网络流日志可快速检测云服务器不可访问的原因是否为安全组设置不合理
网络 ACL	网络流日志可快速检测云服务器不可访问的原因是否为网络 ACL 设置不合理
弹性网卡	网络流日志可采集、分析弹性网卡粒度的流量数据
NAT网关	网络流日志可采集、分析 NAT 网关粒度的流量数据
云联网	网络流日志可采集、分析云联网跨域粒度的流量数据