阿里云
云防火墙

常见问题

文档版本：20190909

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 云防火墙产品试用与售前咨询

如果您在购买云防火墙遇到例如产品功能、产品价格、产品选型等售前问题，或期望进行云防火墙产品试用，可通过钉钉与我们联系。使用钉钉扫描下方的二维码，您将直接获得阿里云云防火墙安全行业专家的指导建议。

在钉钉上扫一扫加我

2 常见问题

云防火墙是否支持经典网络?

南北向防火墙和威胁入侵检测（IPS）功能支持经典网络。东西向微隔离功能可支持VPC，对经典网络不支持。

云防火墙是否支持海外国际站点?

目前版本只支持中国大陆和香港站点，不支持海外国际站点。

是否支持对公网SLB的访问?

对入方向公网SLB的防护，由于网络架构原因暂时不能防御。建议规避方案：采用 DNAT + 内网SLB方案。采用云防火墙后，数据流为： 云防火墙 – DNAT（EIP） – 内网SLB。

是否支持对私网地址的出方向访问控制?

对于出方向的流量，只能针对DNAT或EIP的公网地址进行策略控制，无法对NAT前的私网源IP进行访问控制。

建议规避方案：如需对某个私网地址单独做访问控制，建议针对需要控制的私网源IP地址，单独绑定一个EIP，针对这个EIP做针对性的访问控制策略即可。

是否能针对IPSec的报文进行访问控制?

IPsec 解密后的报文，南北向控制点无法防护。

规避方案：把Ipsec解密的流量当做是东西向流量，采用云防火墙的东西向策略来控制。

是否支持对高速通道的访问控制?

目前云防火墙不支持。可通过安全组来实现对高速通道的访问控制。

网络流量中入方向应用Unknown占比不小，是产品无法识别外网的具体请求吗?

来自互联网的扫描流量很大，该类流量大部分不是标准协议故无法识别为已知协议，显示为unknown。

用户可通过日志 > 流量日志或日志 > 事件日志来观察unknown流量的具体来源与用途。

网络流量分析的全量活动搜索结果中流量访问Top中为什么出现很多未知运营商?

来自海外地区的流量只提供国家级别的识别，如果出入方向存在很多来去海外的流量，运营商会被标识为未知。用户可通过日志 > 流量日志观察到具体IP对应的地区与运营商。

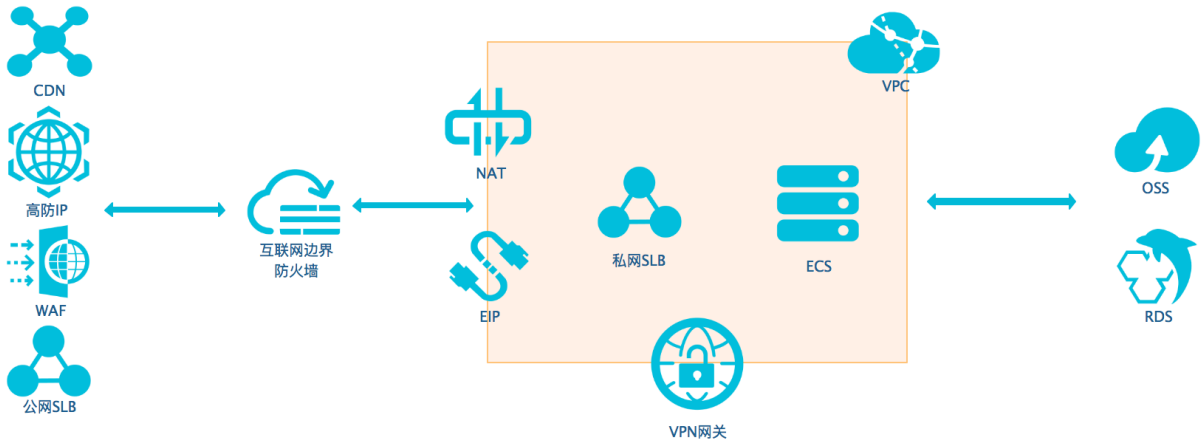
网络流量中出方向应用Unknown占比不小，是否是防火墙不能识别的协议？

出方向的流量可能被目的服务器阻断，发送大量的rst回包，这类包会记录到出方向流量中，如果数量较大，则相应的Unknown占比也较大。遇到这类问题，可以通过日志 > 流量日志来观察unknown流量，来确定是否是出方向流量业务上存在异常行为。

3 云防火墙和其它云产品有怎样的关系?

云防火墙在阿里云网络中的位置

下图展示了部分阿里云产品（包括云防火墙）的逻辑关系。



同WAF、高防等安全产品同时使用

如上图所示，云防火墙防护的是WAF/高防的源站IP。

同CDN产品同时使用

同WAF、高防一样，云防火墙防护的是源站IP。

同OSS、RDS等产品同时使用

目前云防火墙不支持OSS、RDS实例防护，预计将在2019年下半年支持。

同SLB同时使用

SLB分为公网实例和私网实例。云防火墙目前不支持SLB公网实例，支持SLB私网示例+EIP场景防护。

4 云防火墙和安全组有什么差异?

本文档介绍了云防火墙和安全组的主要差异。

安全组是ECS提供的用于设置ECS实例间访问控制的虚拟主机防火墙，是一种分布式的防火墙。

云防火墙是互联网边界防火墙、VPC边界防火墙、主机边界防火墙的统称，为用户提供互联网、虚拟网络、主机三种边界防护。

云防火墙相对安全组的独有功能

- 支持应用级别的访问控制。例如：可以配置HTTP协议放通，其HTTP服务可以运行在任意端口。
- 支持域名级别的访问控制。例如：可以配置只允许所有ECS到`*.aliyun.com`的请求。
- 支持地址簿，可以将一组IP、端口或者具有相同标签的ECS配置为一个地址簿，方便用户进行配置。
- 提供IPS功能，支持常见系统漏洞防护。
- 支持暴力破解防护。
- 提供观察模式，并提供完整流日志，分析阻断数据。

云防火墙相对安全组的增强功能

云防火墙的主机防火墙底层使用了安全组的能力。用户既可以在云防火墙 > 主机防火墙处配置策略也可以在ECS安全组控制台配置策略，两者配置自动保持同步。云防火墙相对安全组提供了一些增强功能：

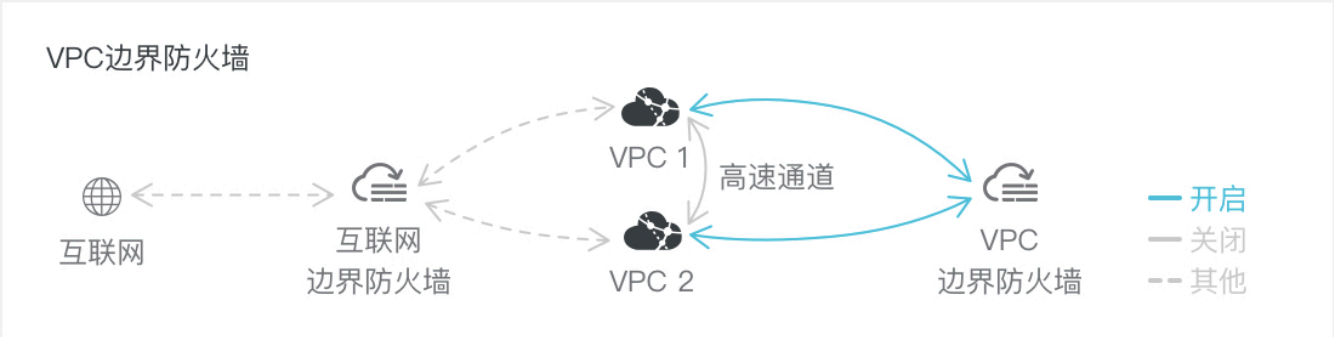
- 支持策略的批量发布。
- 支持策略组初始模板。
- 同应用组配合，自动创建安全组。
- 支持组内ECS实例间默认不通。

为什么会有三种云防火墙

云防火墙是互联网边界防火墙、VPC边界防火墙、主机边界防火墙的统称，为用户提供互联网、虚拟网络、主机三种边界防护。

互联网边界防火墙作用于互联网边界，对所有公网IP统一管控；主机防火墙对应安全组，对ECS间通信进行管控。互联网边界防火墙/主机防火墙原理图和位置如下：

VPC边界防火墙作用于VPC边界，对高速通道流量进行管控。VPC边界防火墙原理图和位置如下：



三种防火墙配合使用，可以让用户精细化地管控数据访问行为，同时也组成了互联网边界-虚拟网络边界-主机边界三层纵深防御体系：

- 对于需要精细化访问控制的需求，云防火墙提供集中式的访问控制，也就是内对外、外对内访问控制策略，提供了应用、域名等精细化访问控制策略，并可以统一管控所有VPC、所有区域，并提供观察模式、地址簿等优化策略配置功能，配置相对简单。
- 对于微隔离的访问控制需求，云防火墙提供分布式的访问控制，目前底层利用的是安全组能力，同时提供所有内部流量的可视能力，帮助用户优化内对内策略。后续会提供策略的观察模式、拦截访问分析、智能策略等能力。

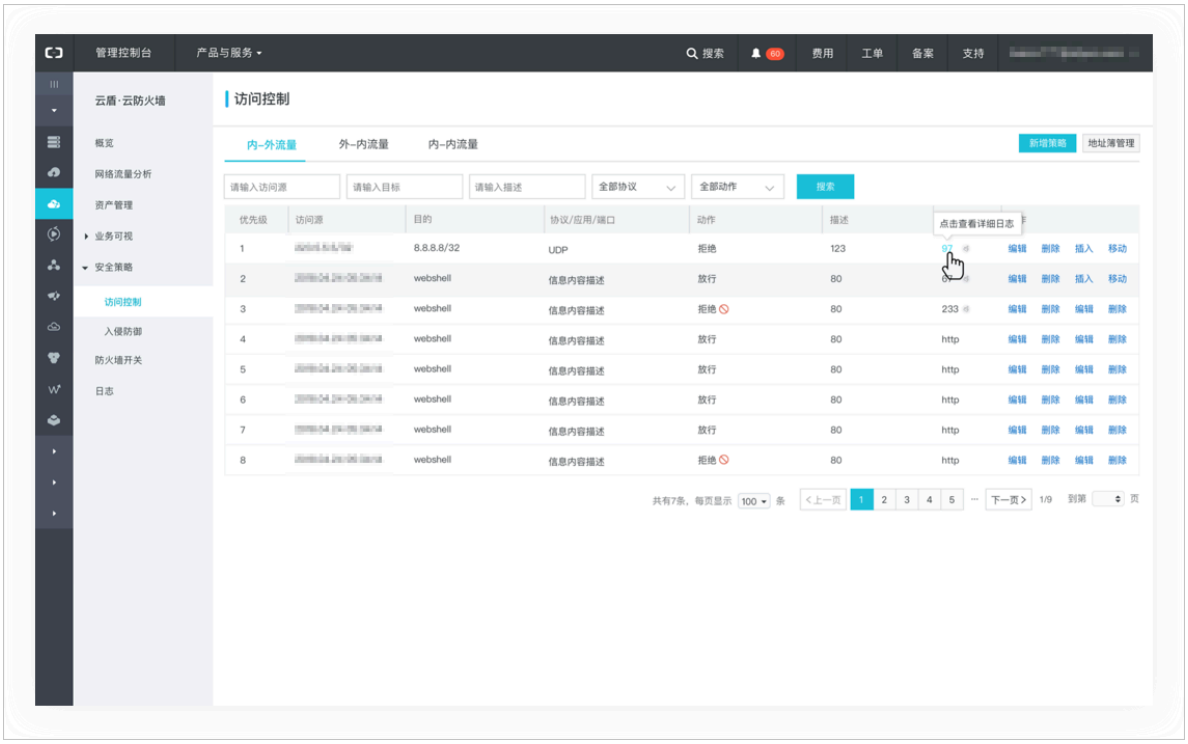
根据网络边界配置防火墙，便于逻辑分层，同时也方便后续维护。如用户只有公网防护需求，就只需要在互联网边界防火墙处配置南北向策略（即内-外或外-内访问控制策略）。如果同时有主机防护需求，可以在主机防火墙处只配置东西向策略（即内-内访问控制策略）。

5 访问控制策略优先级如何判断?

访问控制策略优先级决定了策略生效的顺序。

- 互联网边界防火墙（内-外流量/外-内流量），优先级数字越小优先级越高，越大优先级越低。

  如下图示例中的规则，访问流量进入云防火墙后会依次通过优先级1-8的策略，如果符合放行策略则放行，如果触发拒绝策略则拒绝。互联网边界防火墙优先级是唯一的。



  详细操作说明参见#unique_9。

- 主机防火墙（内-内流量）优先级和安全组一致，优先级数字小的优先级越高，数字越大优先级越低。主机防火墙优先级范围为1-100，优先级可以重复。优先级相同时，动作设置为拒绝的策略优先生效。

6 流量不通时如何排查?

问题描述

流量经过云防火墙时可能会出现以下问题:

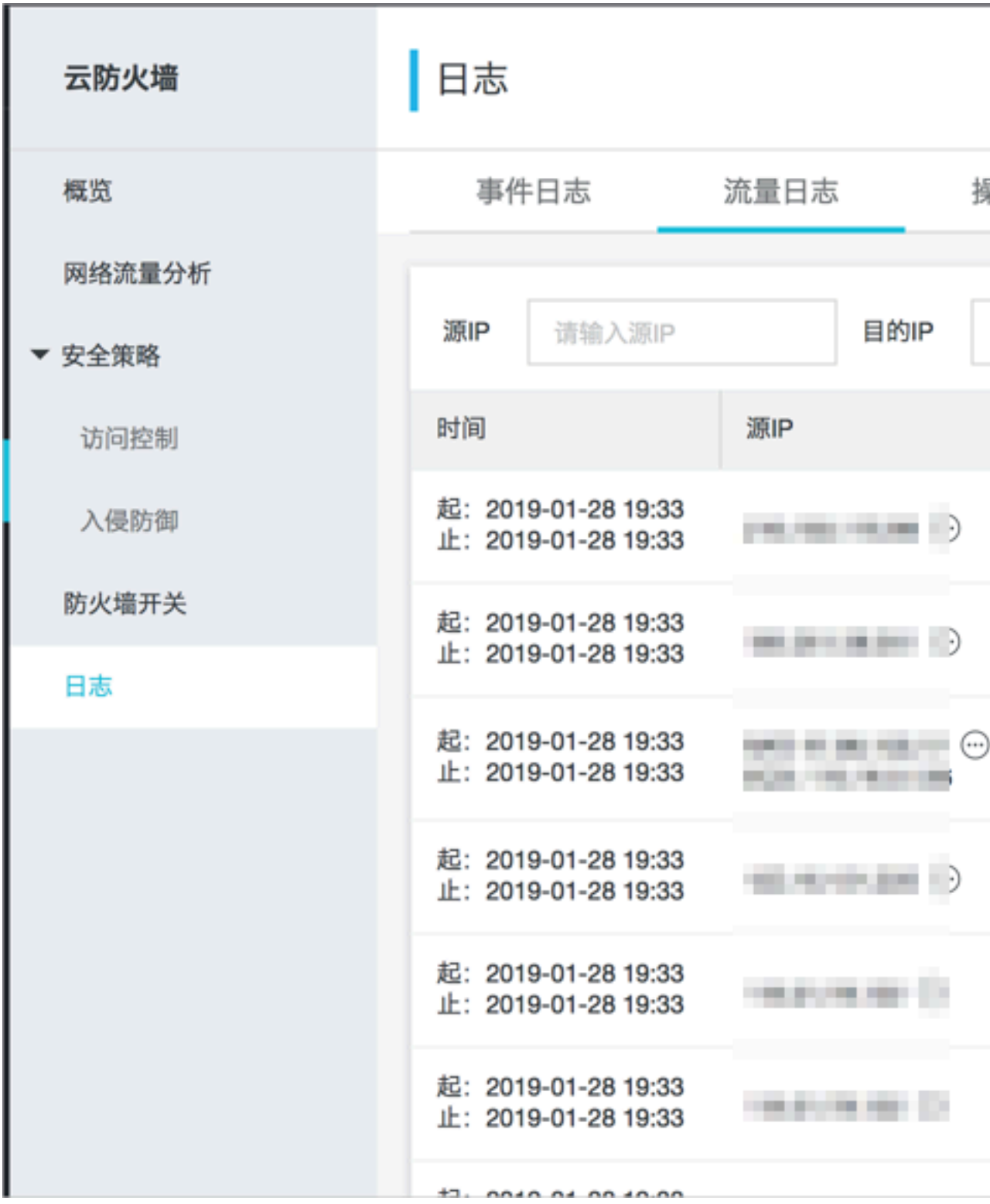
1. 用户无法登录服务器。
2. 用户无法访问服务器上的服务。
3. 服务器无法访问某些外网。

互联网边界防火墙排查步骤

- 确认资产是否开启了互联网边界防火墙，如果未开启，跳过此步骤。

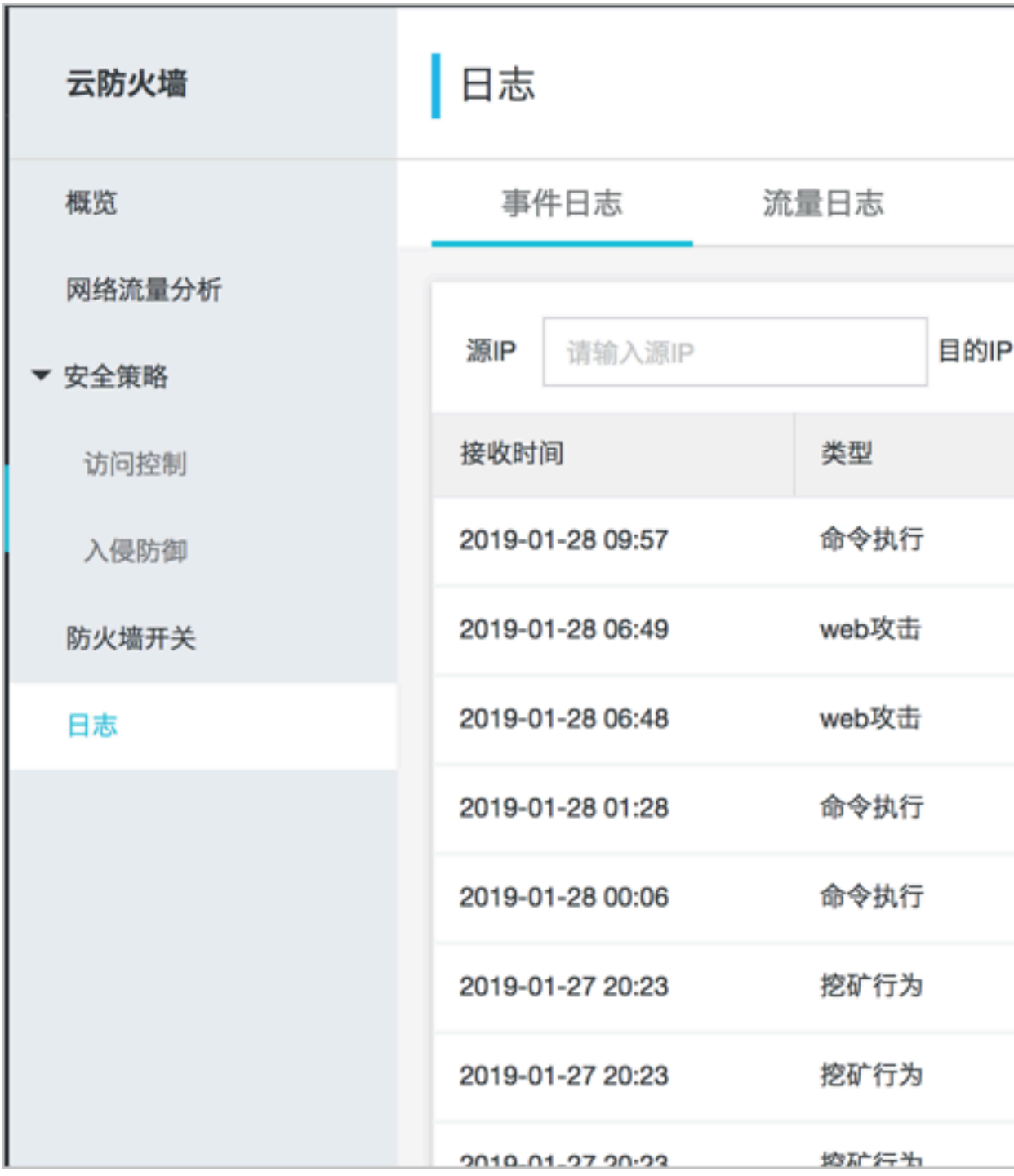
开启边界防火墙操作步骤参见#unique_11。

- 确认日志 > 流量日志中是否有相应的流量记录。



  - 如果不存在流量日志，说明流量还未到达防火墙就被丢弃。

- 如果存在流量日志，且动作为丢弃，说明流量是在主机防火墙处被丢弃，在日志 > 事件日志中查询对应流量，根据判断来源列确认拦截指令来源。



  - 指令来源为访问控制，则需要检查对应访问控制策略配置。
  - 指令来源为基础防御、虚拟补丁或威胁情报时，可以到安全策略-入侵防御页面关闭对应模块。

- 如果存在流量日志，动作为放行或观察，说明流量不是在互联网边界防火墙处被丢弃，需要继续排查主机防火墙/安全组。

主机防火墙/安全组排查步骤

- 登录ECS控制台，点击网络不通的ECS实例，单击导航栏本实例安全组，确认安全组是否放行（授权策略设置为允许）。


launch-advisor-201901
实例详情
本实例磁盘
本实例快照
本实例安全组
本实例安全防护
内网入方向全部规则
内网出方向全部规则
授权策略
协议类型
允许
自定义 TCP
允许
自定义 TCP
允许
自定义 TCP
允许
自定义 TCP
允许
全部 ICMP(IPv4)

如果上述步骤还不能解决您的问题，请提交工单。

7 边界防火墙开关的作用是什么?

您可选择对单个或多个公网IP开启或关闭互联网边界防火墙。

互联网边界防火墙开关开启或关闭时网络流量路径如下图所示:

对于未开启互联网边界防火墙的公网IP，网络流量不经过互联网边界防火墙，只经过主机防火墙/安全组，最终到达用户ECS。

对于开启了互联网边界防火墙的公网IP，流量经过边界防火墙检测和过滤后，再经过主机防火墙/安全组，最终到达用户ECS。

详细操作参见#unique_11。

8 打开/关闭边界防火墙开关有什么影响?

本文档描述了打开或关闭边界防火墙开关所产生的影响。

边界防火墙页面如下图所示:

边界防火墙开关可影响以下功能:

- 概览 > 安全分析页面中,您的资产整体防护等级可能显示为低;资产防护状态模块中受保护资产总数将会减少。
- 概览 > 网络活动页面中,网络流量分析部分图表可能无数据。
- 如果配置了内对外流量或外对内流量访问控制策略,关闭云防火墙开关将会使得该主机对应的策略失效,表现为该策略的命中次数保持不变。
- 关闭防火墙开关,所有流量将不会经过云防火墙,入侵防御功能将会失效。

  IPS即使设置成了观察模式,也不会再去检测这个主机的流量了;如果设置为拦截模式,拦截模式也会失效。
- 关闭防火墙开关后,日志 > 流量日志页面中将不会显示防火墙开关关闭后的流量数据。

详细操作参见#unique_11。

9 为什么有些资产在边界防火墙开关处找不到?

部分云产品资产由于不归属于云防火墙对应账号、不支持开启边界防火墙（如堡垒机），或资产只有私网IP的情况下，您无法在边界防火墙开关处找到对应的资产。

部分资产在边界防火墙开关处找不到可能有以下几点原因：

- 边界防火墙不支持的公网IP类型：SLB公网IP。
- 边界防火墙不支持只有私网IP的资产。
- 该资产不归属于云防火墙对应账号。

边界防火墙支持的公网IP类型：

- EIP（支持绑定到专有网络类型的ECS实例、专有网络类型的私网SLB实例、弹性网卡和NAT网关上）
- NatPublicIP（ECS系统分配的公网IP）

10 使用云防火墙为什么需要授权?

通过使用云防火墙，您可以看到您的云资产在互联网边界的流量请求和响应情况，以及云资产之间的私网业务访问情况，并根据这些数据和分析配置访问控制策略。因此在购买后云防火墙后，需要您的授权以获取云资产的信息。

云防火墙授权内容包括允许云防火墙获取您的ECS实例列表、VPC实例列表、SLB实例列表等权限。

您所拥有的阿里云账号需要满足以下条件之一才可执行云资源访问授权：

- 阿里云主账号
- 拥有管理访问控制权限（AliyunRAMFullAccess）的RAM子账号

授权操作参见#unique_16。

11 金融云基础云防火墙与其它版本的差异

当您有如下需求时，可以考虑将云防火墙基础版升级到高级版或企业版：

- 期望了解云上业务对外开放了哪些公网EIP和哪些端口，应用开放的IP和端口有什么风险。
- 有等保需求，需要保持6个月以上的日志。
- 有基于域名的访问控制需求，期望对失陷主机的主动外联进行控制，控制只允许对外访问某些域名和IP。
- 有FTP、MQTT动态端口协议的应用，需要基于应用进行访问控制。
- 除了杭州金融云，还有其它region的资源需要通过云防火墙防护。

云防火墙杭州金融云基本版与其它商业化版本差异

防火墙基础版（仅杭州金融云）	防火墙高级版
防火墙来源IP+port的访问控制	防火墙来源IP+port的访问控制

高级版（仅金融云）	支持主动外联的检测
	支持基于域名的访问控制
	支持基于应用的访问控制
企业版（仅金融云）	支持主动外联的检测
	支持基于域名的访问控制
	支持基于应用的访问控制

基础版（仅金融云）	
DDoS基础流量检测	
虚拟补丁	
威胁情报	
网络资产梳理	
主动外联活动	
入侵检测活动	

[illegible]（仅[illegible]金融云）
[illegible]PS阻断分析
[illegible]量活动搜索
[illegible]安全日志、流量日志和操作日式，存储6个月

[illegible]（仅[illegible]金融云）

[illegible]扑可视、业务拓扑可视

[illegible]隔离能力（东向西访问控制）

[illegible]region[illegible]共[illegible]region[illegible]）region

[illegible]（仅[illegible]金融云）
[illegible]（互[illegible]网[illegible]墙吞吐量） [illegible]M 可[illegible]
[illegible]，可[illegible]量（ECS）

增强版（仅金融云）	增强版（仅金融云）
最大防护公网IP数量（EIP）	200个	20个
最大策略数	2000条	200条

12 云防火墙的流量日志是否支持导出到第三方系统?

支持。云防火墙产品高级版、企业版和旗舰版支持日志分析功能，并已与阿里云日志服务（SLS）打通。目前云防火墙日志分析功能支持查看并导出互联网流量日志。

您可通过日志分析功能将导出的流量日志文件接入到您的业务系统中，如您的安全运维中心等。

说明:

目前云防火墙已支持互联网流量日志，包括漏洞风险等级和访问控制规则命中结果等数据；暂不支持事件日志和操作日志的导出。

详细日志导出操作参见#unique_20。

13 为什么有来自阿里云的ICMP周期性探测报文?

云防火墙为了保障服务质量，会周期性发送ICMP报文进行探测，该类探测不是扫描攻击，不会对业务造成影响。

其访问源IP在云防火墙地址簿云地址簿中的Source address for SLA monitoring中可以查看到，具体日志数据可以通过访问控制中外对内SLA策略命中次数访问详细日志。