阿里云
云防火墙

产品简介

文档版本：20190816

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 什么是云防火墙?

阿里云云防火墙（Cloud Firewall）是业界首款公共云环境下的SaaS化防火墙，可统一管理互联网到业务的访问控制策略（南北向）和业务与业务之间的微隔离策略（东西向）。内置的威胁入侵检测模块（IPS）支持全网流量可视和业务间访问关系可视，是用户业务上云的第一个网络安全基础设施。

2 技术原理

云防火墙是阿里云云盾团队结合云的部署便捷、弹性扩展等技术优势，为云上客户量身定制的融合访问控制、业务隔离、流量识别等功能的网络安全产品。

云防火墙主要由以下两个控制模块组成：

- 南北向流量控制模块：主要用于实现互联网到主机间的访问控制，支持4-7层访问控制。
- 东西向流量控制模块：主要是利用安全组对主机之间的交互流量进行控制，实现4层访问控制。

3 功能特性

阿里云云防火墙是业界首款云平台SaaS化的防火墙，可统一管理南北向和东西向的流量，提供流量监控、精准访问控制、实时入侵防御等功能，全面保护您的网络安全。

云防火墙支持以下功能：

- 实时流量监控：
  - 可对主动外联行为进行监控。
  - 支持对互联网访问流量进行分析。
  - 支持内网ECS互访流量分析。
  - 支持业务可视，让您全面了解资产的信息和访问关系，从而及时发现异常流量。
- 访问控制：
  - 支持互联网应用访问控制（南北向）。
  - 支持内网ECS之间的微隔离（东西向）。
  - 同时控制入流量和出流量的访问。
  - 支持基于域名的访问控制，严格控制主动外联的出流量。
  - 支持主动外联分析，帮助您主动发现主机的异常行为。
- 实时防御：
  - 支持入侵防御功能并同步进行智能阻断。支持被阻断访问分析，识别被云防火墙和IPS阻断的网络流量。
  - 威胁情报联动：同步阿里云全网的恶意IP，如恶意访问源、扫描源、中控服务等，对威胁和入侵做到提前防御。
  - 内置云平台长期攻防实战中积累的入侵防御规则，威胁识别率高、误报率小。
  - 支持虚拟补丁，无需在业务系统上安装补丁即可实时修复。可对热门漏洞、高危0-day和N-day的利用进行精准防护。
- 行为回溯：
  - 提供事件日志，可实时查看被入侵防御模块检测和拦截到的威胁或入侵事件。
  - 提供流量日志，可查看经过云防火墙的所有流量数据。您可在威胁事件发生的时候通过查看流量日志进行流量和访问源分析，并查看配置的访问控制策略是否生效。
  - 提供系统操作日志，可查看云防火墙所有的配置和操作记录。
  - 日志可保存6个月，符合网络安全法和等保规范要求。

功能列表

4 产品优势

阿里云云防火墙是业界首款云平台SaaS化的防火墙，可统一管理南北向和东西向的流量，全面保护您的网络安全。阿里云云防火墙操作简便、即开即用，支持精准访问控制和全网流量可视化。

简便易用、防火墙即服务

云防火墙采用SDN技术、首次在公共云提供SaaS化的防火墙方案，用户购买后在控制台开通云防火墙，进行简单的策略配置后即可使用。无需传统防火墙的镜像安装、路由设置等复杂基础系统和网络配置操作，用户也无需关注容灾、扩容或接入等问题。

支持平滑扩展

云防火墙采用了集群部署的模式，支持性能的平滑扩展，针对单个IP的防护流量可达2Gbps；防护流量超过2Gbps时云防火墙支持定制。

系统稳定可靠

采用双Available Zone （AZ，可用区）部署，任意一台服务器或者任意一个AZ故障时都不会导致防火墙故障。

一键bypass目标IP，可帮助您在运维时实现快速诊断。

统一策略管理

云防火墙为您的资产提供了完整的南北向和东西向访问控制能力，帮助您的业务建立完整的访问控制和安全隔离能力。

通过云防火墙，您可以在网络层面控制对ECS/RDS/SLB等常用云资产的访问，解决对云资产的异常访问问题。

实时入侵防御

内置威胁检测引擎，可同步更新全网威胁情报，对来自互联网的威胁进行实时检测和阻断。

业务关系可视

云防火墙通过拓扑图直观地展现资产以及资产的访问关系。无需配置，开通服务后就可了解业务的分区、分组、资产、资产间的访问关系，以及用户流量的聚类分析。支持流量可视分析，最大程度保证策略的正确性。

满足等保合规要求

满足等保要求中的边界防护和访问控制等要求。

5 应用场景

云防火墙是用户上云后的首个安全组件，支持全网流量识别、统一策略管控、入侵检测、日志等核心功能。

云防火墙不仅可以防护从互联网到业务的访问，同时还能控制业务到互联网的主动外联访问，并对业务和业务间的访问进行控制。

云防火墙适用于以下应用场景：

- 互联网业务防护：例如某金融用户除了HTTP业务外，还有其他类型业务暴露在互联网上。用户需要使用入侵检测模块（IPS）进行防护。
- 主动外联防护：例如某政府行业用户，除了关注从互联网到业务的防御，也同时关注业务主动外联的分析，以判断哪些主机已经处于风险状态，并对这些异常行为进行实时阻断，规避潜在的风险。
- 微隔离防护：例如某电商客户，虽然都是HTTP业务、并采用了Web应用防火墙进行防护，但期望能对不同的业务间进行安全隔离，增强整体的网络控制能力，避免因为某个ECS安全风险而导致整个云上业务产生风险。

6 云防火墙词汇表

互联网边界防火墙

互联网边界防火墙是指用于检测互联网和云上资产间通信流量的防火墙，是一种集中式管理的防火墙。互联网边界防火墙生效在互联网和用户主机之间，原理图示如下：

互联网边界防火墙内置威胁入侵防御模块，支持失陷主机检测、主动外联行为的阻断、业务访问关系可视等功能。互联边界防火墙是一款SaaS化防火墙，支持一键开启防护，无需复杂的网络接入配置和镜像文件安装，缺省集群化部署，支持性能的平滑扩展。

VPC边界防火墙

VPC边界防火墙是指用于检测两个VPC间通信流量的防火墙，是一种分布式防火墙。VPC边界防火墙生效在两个用户VPC之间，原理图示如下:

VPC边界防火墙仅支持部署在有高速通道联通的两个VPC间，或加入到同一个云企业网的两个VPC间。VPC边界防火墙不会默认存在，需要用户指定两个VPC进行创建。

安全组/主机防火墙

安全组是ECS提供的分布式虚拟主机防火墙，具备状态检测和数据包过滤功能，用于设置ECS实例间的网络访问控制。安全组是由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。在创建实例的时候需要指定安全组，每个实例至少属于一个安全组。

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安全组控制台配置策略，两者配置自动保持同步。

主动外联

主动外联是指阿里云主机主动访问外部IP的连接分析，可以帮助您及时发现可疑主机。

入侵检测

入侵检测是一种监控网络传输，检查是否有可疑活动的系统，在检测到可疑事件时发出告警或者采取主动反应措施。云防火墙集成阿里云近十年检测防御能力积累，对经过云防火墙的流量进行实时分析、统计，智能发现失陷主机、阻断异常网络活动。

开放应用/开放端口/开放公网IP

开放应用指用户暴露在互联网上应用，如HTTP、SSH等。

开放端口指用户暴露在互联网上的端口，如80、22等。

开放公网IP指用户暴露在互联网上的资产的公网IP。

目前云防火墙支持识别以下几种资产的公网IP：

- 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）

应用组

应用组是东西向业务可视中提供的相同/相似服务的应用集合，如所有部署了MySQL的ECS可以归属到同一个DB应用组。

业务区

业务区是东西向业务可视中构成用户某个业务的各个应用组的集合，如门户网站业务区将包含Web应用组、DB应用组等。

高危应用组/高危业务区

高危应用组指开放了高危端口（如445端口）的应用的集合。每一个高危端口会独立产生一个高危应用组。

高危业务区是高危应用组的集合。

高危业务区/高危应用组可以帮助用户发现哪些ECS开放了不当的高危端口以及具体哪些ECS访问了高危端口。

目前高危业务区由云防火墙自动创建和识别。

依赖区/被依赖区

依赖区/被依赖区是东西向业务可视中提供的抽象概念，是指两个业务区的访问关系。如业务区A访问了业务区B，那么我们称业务区B是业务区A的依赖区，而业务区A是业务区B的被依赖区。

首次流量

首次流量指源IP到目的IP的访问流量在统计周期内第一次出现。您可以根据首次流量出现的时间、源目的IP等信息，进一步排查首次流量出现的原因。通常情况下首次流量由新业务上线或者入侵造成。

地址簿

为了方便的引用IP地址或端口信息，实现灵活配置，云防火墙支持将多个IP地址或者多个端口指定成一个地址簿。在配置时，只需要引用该地址簿即可实现对多个IP地址或端口的批量配置。

云防火墙目前支持三类地址簿：

- IP地址簿：用户可以配置一组IP。
- 端口地址簿：用户可以配置一组端口。
- ECS标签地址簿：用户可以指定一组ECS标签，云防火墙自动将具有这些标签的ECS公网IP放到一个地址簿中。

地址簿还具有以下特点：

- 云防火墙内置一些全局地址簿，全局地址簿用户不可以编辑也不可以删除。
- 多个地址簿可以包含同一个IP地址或端口。
- 地址簿内IP或端口变动，会自动生效于访问控制策略。