阿里云
云防火墙

产品简介

文档版本：20181115

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。
斜体	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 技术原理

云防火墙是基于分布式架构的安全产品，解决了云上业务快速变化带来的安全边界模糊甚至无法定义的问题。

基本原理

云防火墙的基本原理是通过对您的业务流量进行学习和展示，从而引导对您快速完成业务的分区、分组，以及安全策略的定义。

- 云防火墙会如实的还原您的业务流量（服务器信息、服务器之间的访问关系），并通过一系列基于算法的数据分析，让您可以快速找到自己想要看见的信息（服务器、访问连接）。
- 云防火墙会引导管理员对流量进行逐一排查和确认，最终将原本无序的业务进行分区、分组、并部署安全策略。
- 云防火墙会持续进行业务流量的主动学习和全局展示，以保持业务的有序状态。

2 功能特性

云防火墙可统一管理互联网与业务间（南北向）、业务和业务间（东西向）的隔离以及访问控制，并内置了威胁入侵检测模块（IPS），全面保护您的网络安全。

- 支持防火墙安全控制，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。
- 主持主动外联分析，帮助您主动发现主机的异常行为。
- 支持入侵防御、智能阻断入侵，无需复杂的规则配置。
- 支持安全事件日志、流量日志和系统日志。日志可保存6个月，符合网络安全法和等保规范要求。
- 支持互联网到业务的访问流量分析。
- 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。
- 业务可视，帮助您全面了解资产的信息和访问关系。
- 云防火墙的策略部署提供了观察模式和一键全通两个功能，保障在测试阶段和突发情况下的业务稳定性。

3 产品优势

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。购买后在控制台开通云防火墙服务，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，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。

支持一键关闭单个或多个资产的云防火墙，可帮助用户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。

支持在网络层面对ECS/RDS/SLB等常用云资产进行访问控制，发现和处理对云资产的异常访问。

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。开通服务后通过简单的策略配置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。

4 应用场景

云防火墙适用于以下应用场景：

- **实现微隔离**：原来为了防止业务出现中断而不得不开放的端口，云防火墙可以帮助您实现精细化的微隔离（业务分区、角色分组），缩小了攻击面，降低安全隐患。
- **帮助甄别流量是否安全**：例如HTTP流量是否都已切换为HTTPS的流量？例如连接TCP 3306（MySQL的业务端口）的流量是否有来自互联网的？这些信息，在云防火墙的流量视图中，一目了然。
- **服务器变更，对业务是否造成了影响**：服务器的迁移和下线的时候，可以通过云防火墙先看看是否还有相关流量，以判断是否可以安全的变更。
- **帮助快速扩容**：云防火墙去IP化的策略定义方式，能够在业务快速增长时，保持策略不发生频繁变更。例如双11的时候，只需要赋予一批新购的服务器相同的角色，策略无需任何修改，即可完成扩容。
- **流量可视，快速运维**：以前想要了解出入服务器的连接，只能通过抓包或tcpdump。云防火墙通过流量线条的方式，将相关信息可视化的呈现。
- **是否存在端口滥用**：不同的业务开发部门，可能导致服务器提供同一服务（相同应用和进程），却使用了不同的业务端口，这样既浪费了端口资源，也不便于运维。通过流量的可视，云防火墙可以清晰的甄别出此种情况。