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，是您业务上云的第一个网络安全基础设施。

**云防火墙支持防护的范围**

云防火墙可以防护以下云资产或流量：

* 互联网方向：ECS公网IP、SLB EIP、部分SLB公网IP（详见以下说明）、HAVIP、EIP、ECS EIP、ENI EIP、NAT EIP。

**说明** 阿里云提供公网和私网两种类型的负载均衡（SLB）服务。由于历史网络架构的原因，部分公网SLB不支持云防火墙引流，推荐您采用私网SLB加EIP的方案（详细内容请参见[绑定EIP](https://help.aliyun.com/document_detail/86105.html#task-bxf-ctt-j2b)），将流量牵引到云防火墙上进行防护。

* VPC间：已使用云企业网或高速通道连接VPC间通信的流量。

**功能列表**

下表介绍了云防火墙的功能特性和支持的版本信息。

| **应用场景** | **功能名称** | **描述** | **支持的版本** | **相关文档** |
| --- | --- | --- | --- | --- |
| 云上网络访问流量分析与攻击感知 | 概览 | 提供已开启和未开启的防御能力总览，并为您展示最近7天访问流量统计数据和已检测出的安全风险统计数据。 | 所有付费版本 | [概览](https://help.aliyun.com/document_detail/150636.html#concept-2393024) |
| 访问控制 | 互联网边界防火墙 | 支持互联网双向访问控制（南北向）；支持基于域名的访问控制，严格控制主动外联的出流量。 | 所有付费版本 | [互联网边界防火墙（内外双向流量）](https://help.aliyun.com/document_detail/101318.html#concept-xx1-wgr-ggb) |
| VPC边界防火墙 | 支持VPC间流量访问控制。 | 仅企业版、旗舰版 | [VPC边界防火墙](https://help.aliyun.com/document_detail/101319.html#concept-vgy-wgr-ggb) |
| 主机边界防火墙 | 支持内网ECS之间的微隔离（东西向）。 | 所有付费版本 | [主机边界防火墙（ECS实例间）](https://help.aliyun.com/document_detail/90631.html#concept-lxf-5k4-cfb) |
| 网络流量实时监控和分析 | 主动外联活动 | 实时监控云资产主动外联的行为。 | 所有付费版本 | [主动外联活动](https://help.aliyun.com/document_detail/90630.html#concept-vc3-qk4-cfb) |
| 互联网访问活动 | 支持云上网络访问流量统计和分析。 | 所有付费版本 | [互联网访问活动](https://help.aliyun.com/document_detail/97264.html#task-1939614) |
| VPC访问活动 | 实时监控VPC专有网络之间的流量情况，帮助您实时获取VPC网络流量数据，及时发现和排查异常流量。 | 仅企业版、旗舰版 | [VPC访问活动](https://help.aliyun.com/document_detail/133804.html#task-1925821) |
| 失陷感知 | 由威胁检测引擎实时检测入侵活动及其详细信息并提供对应的处置方案。 | 所有付费版本 | [失陷感知](https://help.aliyun.com/document_detail/92937.html#task-1939609) |
| IPS拦截记录 | 云防火墙提供入侵防御功能并同步进行智能阻断，提供被阻断的访问流量分析，帮助您有效识别被云防火墙阻断的网络流量。 | 所有付费版本 | [IPS拦截记录](https://help.aliyun.com/document_detail/92936.html#concept-int-klb-kfb) |
| 全量活动搜索 | 支持基于过滤条件对经过云防火墙的访问流量进行搜索。 | 所有付费版本 | [全量活动搜索](https://help.aliyun.com/document_detail/92939.html#task-1939611) |
| 入侵防御 | 漏洞攻击防护 | 实时检测可被网络侧攻击利用的漏洞，并提供针对此类漏洞的攻击防御能力。 | 所有付费版本 | [漏洞攻击防护](https://help.aliyun.com/document_detail/181201.html#task-1940469) |
| 入侵防御 | * 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漏洞的利用进行精准防护。 | 所有付费版本 | [入侵防御开关](https://help.aliyun.com/document_detail/90980.html#task-ocy-lxd-dfb) |
| 日志 | 日志审计 | 提供日志审计和行为回溯，详细介绍如下：   * 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。 | 所有付费版本 | [日志审计](https://help.aliyun.com/document_detail/90633.html#concept-z4k-xk4-cfb) |
| 日志分析 | 实时地自动采集并存储（存储时长可达6个月）出、入方向的流量日志并进行分析；支持基于特定指标定制准实时的监测与告警，确保在关键业务发生异常时能及时响应。 | 所有付费版本 | [开通日志服务](https://help.aliyun.com/document_detail/113185.html#concept-pzr-rxj-hhb) |
| 常用网络流量检测工具 | 工具箱 | 提供网络抓包、策略回滚、安全组配置检查等功能，帮助您全面了解经过云防火墙的网络流量。 | * 安全组配置检查和等保合规检测功能支持免费版和所有付费版本。 * 网络抓包、策略备份与回滚功能仅支持付费版本。 | [策略回滚](https://help.aliyun.com/document_detail/170363.html#task-2519501)  [网络抓包](https://help.aliyun.com/document_detail/140840.html#task-2315678)  [安全组配置检查](https://help.aliyun.com/document_detail/178389.html#task-1918215) |
| 业务可视 | 安全组可视、应用分组可视 | 支持业务可视，帮助您全面了解云资产的信息和访问关系。 | 所有付费版本 | [安全组可视](https://help.aliyun.com/document_detail/120149.html#task-1938151)  [应用分组可视](https://help.aliyun.com/document_detail/120148.html#concept-337352) |
| 自定义分组 | 支持通过自定义分组建立云资产的应用和应用组、业务区之间的关系。 | 所有付费版本 | [自定义分组](https://help.aliyun.com/document_detail/120147.html#concept-337351) |

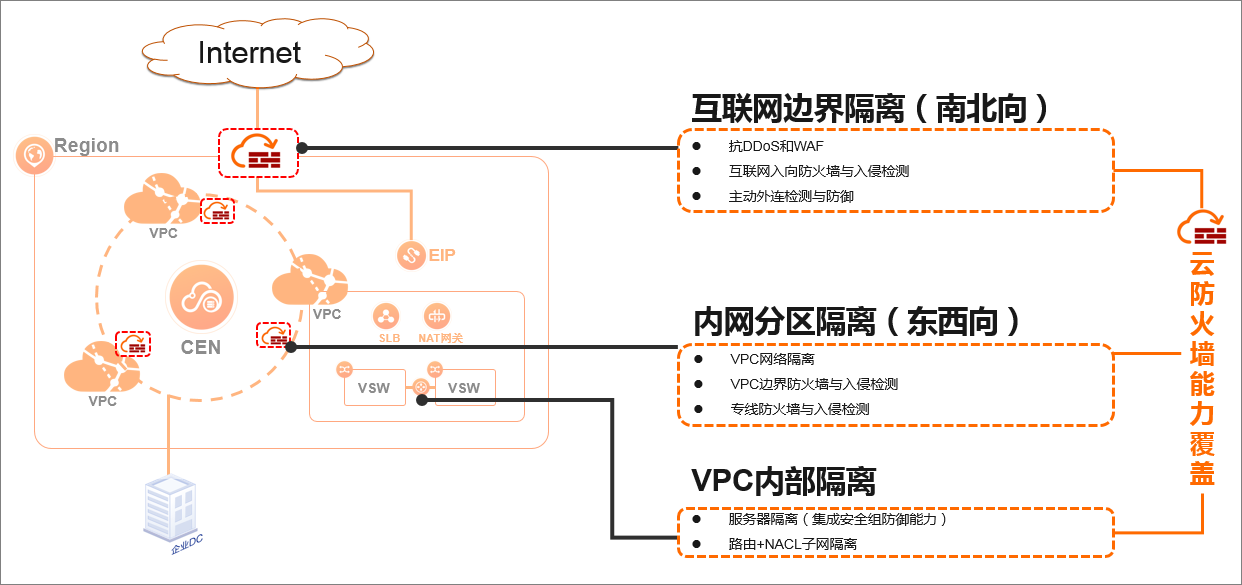
# 应用场景

更新时间：2020-09-26 00:52:27

[**本页目录**](javascript:void(0))

* [互联网边界访问控制](https://help.aliyun.com/document_detail/90223.html?spm=a2c4g.11186623.6.548.7b973fd69r2vr2#title-ti7-e0u-dzq)
* [内网访问控制](https://help.aliyun.com/document_detail/90223.html?spm=a2c4g.11186623.6.548.7b973fd69r2vr2#title-yw8-g51-3lc)
* [VPC边界访问控制](https://help.aliyun.com/document_detail/90223.html?spm=a2c4g.11186623.6.548.7b973fd69r2vr2#title-rgk-5sd-4gm)
* [入侵防御](https://help.aliyun.com/document_detail/90223.html?spm=a2c4g.11186623.6.548.7b973fd69r2vr2#title-73x-l7j-raj)
* [流量可视化](https://help.aliyun.com/document_detail/90223.html?spm=a2c4g.11186623.6.548.7b973fd69r2vr2#title-s04-uc7-q3u)
* [等保合规](https://help.aliyun.com/document_detail/90223.html?spm=a2c4g.11186623.6.548.7b973fd69r2vr2#title-504-kyu-v2l)

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流量，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。[](http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/6335910061/p166793.png)

## 互联网边界访问控制

对出、入互联网的访问流量进行管控，拦截来自互联网的攻击和威胁，例如黑客入侵、挖矿和恶意流量等。

## 内网访问控制

对内网中ECS服务器之间的访问流量进行管控，对不同的业务进行安全隔离，避免因某个ECS存在安全风险从而对整个云上业务产生安全威胁。

## VPC边界访问控制

对VPC间的访问流量进行管控，实现VPC的分区防御。

## 入侵防御

对云资产主动外联的行为、互联网访问流量和内网ECS互访流量进行检测和分析，帮助您实时了解网络流量动态，以判断哪些云资产已经处于风险状态，并对这些异常行为进行实时阻断，防御潜在的风险。

## 流量可视化

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。

## 等保合规

存储云资产6个月以上的访问日志，助力网站符合等保合规要求。

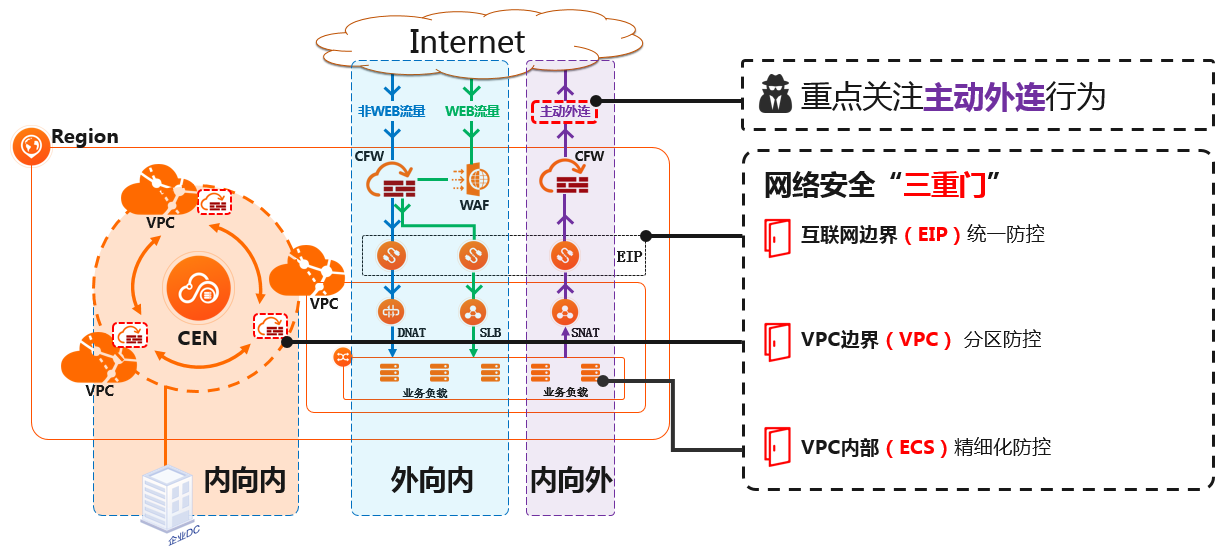
# 阿里云网络安全最佳实践

更新时间：2020-09-22 20:10:40

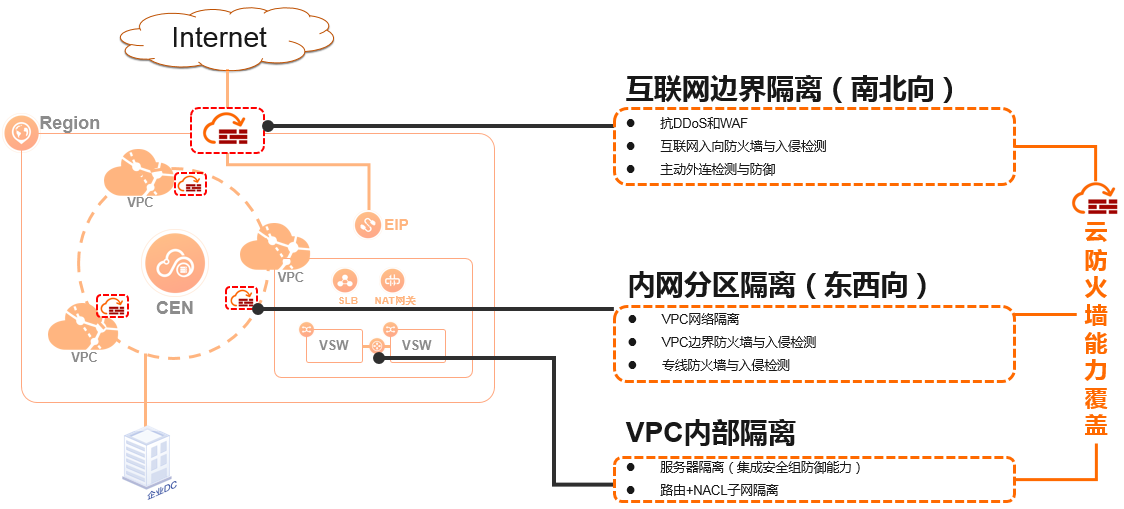
[**本页目录**](javascript:void(0))

* [安全区域边界防护](https://help.aliyun.com/document_detail/184460.html?spm=a2c4g.11186623.6.549.6bd839a7MXxkxz#h2-url-1)
* [“层次化”的网络防御能力](https://help.aliyun.com/document_detail/184460.html?spm=a2c4g.11186623.6.549.6bd839a7MXxkxz#title-fty-o1w-x3c)
* [网络安全组件对比](https://help.aliyun.com/document_detail/184460.html?spm=a2c4g.11186623.6.549.6bd839a7MXxkxz#title-kf7-biz-en0)

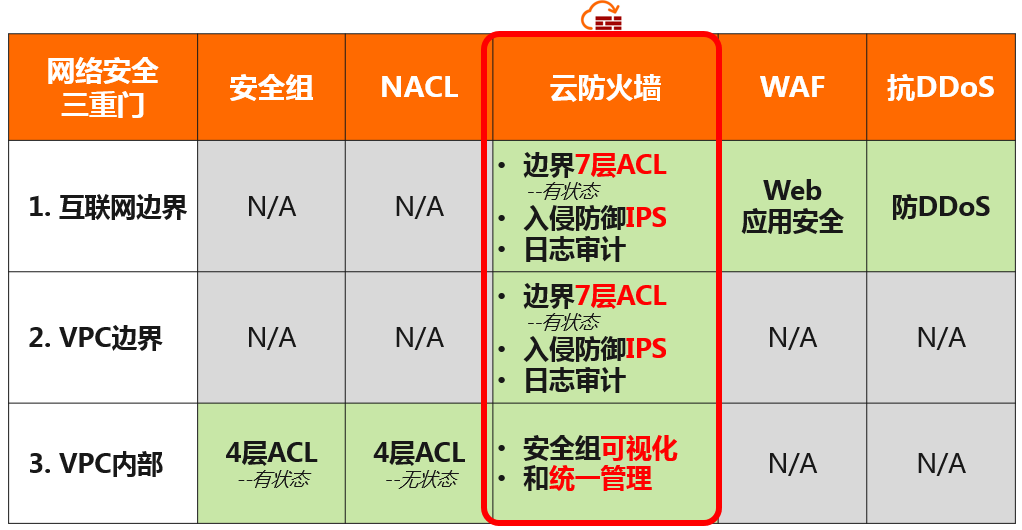
## 安全区域边界防护

云防火墙提供云上网络防护三重门，即内到内、外到内、内到外方向流量的管控，满足等保合规对于安全区域边界防护的要求。[](http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/6756770061/p169303.png)

## “层次化”的网络防御能力

云防火墙提供层次化的网络防御能力，实现互联网边界、内网ECS服务器之间和VPC之间的安全隔离。[](http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/6756770061/p169300.png)

## 网络安全组件对比

云防火墙互联网边界和VPC边界支持7层访问控制，全面防护网络安全。[](http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/6756770061/p169299.png)

[上一篇：应用场景](https://help.aliyun.com/document_detail/90223.html)