云防火墙

产品介绍

文档版本 19

发布日期 2025-01-07

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 什么是云防火墙

云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。

智能防御

CFW集成华为云/安全能力积累和华为全网威胁情报，提供AI入侵防御引擎对恶意流量实时检测和拦截，与安全服务全局联动，防御木马蠕虫、注入攻击、漏洞扫描、网络钓鱼等攻击。

灵活扩展

CFW可对全流量进行精细化管控，包括互联网边界防护、跨VPC的流量，防止外部入侵、内部渗透攻击和从内到外的非法访问；同时，带宽/EIP/安全策略等关键性能规格可无限扩展（根据客户需求灵活调整底层虚拟机的资源和数量，按需设置CPU和内存等资源规格），集群部署高可靠，满足大规模流量的安全防护。

极简应用

作为云原生防火墙，华为云防火墙支持一键开启，多引擎安全策略一键导入，资产自动秒级盘点，操作页面可视化呈现，大幅提高管理和防护效率。

支持的访问控制策略

- 基于五元组的访问控制。即源IP地址、目的IP地址、协议号、源端口、目的端口。
- 基于域名的访问控制。
- 基于IPS（intrusion prevention system，入侵防御系统）设置访问控制。IPS支持观察模式和阻断模式，当您选择阻断模式时，云防火墙根据IPS规则检测出符合攻击特征的流量进行阻断。
- 支持对IP地址组、 黑名单、白名单设置ACL访问控制策略。

2 功能特性

云防火墙提供了“基础版”、“标准版”、“专业版”供您使用，包括访问控制、入侵防御、流量分析以及日志审计等功能。

表 2-1 功能特性

功能项	功能描述
总览	提供防火墙实例基本信息、资源防护总览、统计信息等内容。
资产管理	管理、查看弹性公网IP和VPC的相关数据及信息。
访问控制	• 支持基于IP、域名、地域等方式对互联网边界和VPC边界流量进行访问控制。 • 支持通过“策略助手”快速查看防护规则的命中情况，及时调整防护规则。

功能项	功能描述
攻击防御	● 入侵防御（IPS）：结合多年攻防积累的经验规则，针对访问流量进行检测与防护，覆盖多种常见的网络攻击，有效保护您的资产。 – 基础防御规则库：根据内置的IPS规则库，提供威胁检测和漏洞扫描。支持检测流量中是否含有网络钓鱼、特洛伊木马、蠕虫、黑客工具、间谍软件、密码攻击、漏洞攻击、SQL注入攻击、XSS跨站脚本攻击、Web攻击；以及检测是否存在协议异常、缓冲区溢出、访问控制、可疑DNS活动及其它可疑行为。 **说明** 基础防御规则库支持手动修改防护动作。 基础防御规则库支持通过“规则ID”、“特征名称”、“风险等级”、“更新年份”、“CVE编号”、“攻击类型”、“规则组”、“当前动作”查询规则信息。 – 虚拟补丁规则库：在网络层级为IPS提供热补丁，实时拦截高危漏洞的远程攻击行为，同时避免修复漏洞时造成业务中断。虚拟补丁规则库中展示新增的IPS规则；防火墙新增IPS规则时，会先进入虚拟补丁规则库中，防护一段时间后合入IPS规则库中。 – 自定义IPS特征：当IPS规则库不满足使用时，CFW支持自定义IPS特征规则，添加后，CFW将基于签名特征检测数据流量是否存在威胁。 **说明** 自定义IPS特征支持添加HTTP、TCP、UDP、POP3、SMTP、FTP的协议类型。 ● “敏感目录扫描防御”：防御对用户主机敏感目录的扫描攻击。 ● “反弹Shell检测防御”：防御网络上通过反弹shell方式进行的网络攻击。 ● 病毒防御（Anti-Virus，AV）：通过病毒特征检测来识别和处理病毒文件，避免由病毒文件引起的数据破坏、权限更改和系统崩溃等情况发生，有效保护您的业务安全。 病毒防御功能支持检测HTTP、SMTP、POP3、FTP、IMAP4、SMB的协议类型。 ● “安全看板”：快速查看攻击防御功能的防护信息，及时调整IPS防护。
流量分析	为您展示以下流量统计情况。 ● 入云流量：互联网访问云主机的流量统计。 ● 出云流量：云主机主动访问互联网的流量统计。 ● VPC间访问：VPC间的出入流量统计。
日志审计	支持入侵攻击事件日志、访问控制日志、流量日志。其中： ● 攻击事件日志：入侵攻击事件的详细信息。 ● 访问控制日志：可以查看哪些访问放行，哪些访问被阻断的详细信息。 ● 流量日志：可以查看具体某个业务的访问流量信息。 CFW支持全量日志功能，您可以将攻击事件日志、访问控制日志、流量日志记录到华为云的云日志服务（Log Tank Service，简称LTS）

功能项	功能描述
系统管理	● 告警通知：您可以通过云防火墙服务对攻击日志和流量超额预警进行通知设置。开启告警通知后，CFW可将IPS攻击日志和流量超额的预警信息通过您设置的接收通知方式（例如邮件或短信）发送给您。 ● 网络抓包：帮助您定位网络故障和攻击。 ● 多账号管理：一个账号下的云防火墙实例同时防护多个账号的EIP资源。 ● DNS配置：通过域名服务器解析并下发IP地址。 ● 安全报告：生成日志报告，及时掌握资产的安全状况数据。

表 2-2 引擎特性

名称	主要功能描述	支持协议	支持场景
防火墙引擎	用户流量先经过负载均衡组件分发给租户防火墙引擎，进行安全检测与防护后，再将流量送至目标ECS。检测功能丰富，阻断策略灵活。	TCP、UDP、ICMP、Any	可以支持互联网边界和VPC边界的防护。

3 应用场景

外部入侵防御

通过云防火墙，对已开放公网访问的服务资产进行安全盘点，可一键开启入侵检测与防御。

主动外联管控

云防火墙支持基于域名的访问控制，可对主动外联行为进行管控。

VPC 间互访控制（专业版支持）

云防火墙支持VPC间流量的访问控制，实现内部业务互访活动的可视化与安全防护。

等保合规

云防火墙可满足《网络安全等级保护2.0》中对区域边界防护、网络入侵防范、网络访问控制、安全日志审计等检查要求。

4 服务版本差异

云防火墙提供了“基础版”、“标准版”、“专业版”供您使用，包括访问控制、入侵防御、流量分析以及日志审计等功能。

详细的功能介绍请参见**功能特性**，具体差异请参见**表 版本差异说明**。

表 4-1 版本说明

版本	计费模式	防护对象	版本说明
基础版	包周期	EIP	• 提供EIP的精细化访问控制策略配置 • 满足日志查询需求
标准版	包周期	EIP	• 满足等保需求 • 提供网络入侵、主机失陷等网络安全防护
专业版	• 按需 • 包周期	• EIP • VPC	• 满足等保或重保需求 • 提供网络入侵、主机失陷、内部网络互访等网络安全防护。

表 4-2 版本差异说明

功能		基础版（新）①	标准版	专业版（包周期）	专业版（按需）
防护对象	IPv4	√	√	√	√
	IPv6	×	×	×	×
防护规格	防护的公网IP（EIP）数量	20个（不可扩容）	20个（可扩容，最大扩容至2000个）	50个（可扩容，最大扩容至2000个）	1000个（上限）

功能		基础版（新）①	标准版	专业版（包周期）	专业版（按需）
	防护的VPC数量	×	×	2个（可扩容，最大扩容至1000个）	20个（上限）
	互联网边界防护带宽	10Mbps（不可扩容）	10Mbps（可扩容，最大扩容至50,000Mbps）	50Mbps（可扩容，最大扩容至50,000Mbps）	1 Gbps
	VPC边界防护带宽	×	×	200Mbps（随VPC数量扩容）	
访问流量控制	公网资产ACL访问控制（基于IP、域名、域名组、地理位置等）	√（仅支持通过Host或SNI字段匹配策略）	√	√	√
	南北向流量防护，统一隔离防护云上资产在互联网的暴露风险（例如EIP）	√	√	√	√
	南北向流量审计，日志查询	√（仅支持访问控制日志和流量日志）	√	√	√
	东西向流量防护，VPC间的资产保护、全流量分析	×	×	√	√
	东西向流量监控，实时获取VPC间流量数据	×	×	√	√
防护策略	入侵防御IPS	×	√	√	√
	自定义IPS特征库	×	×	√	√
	虚拟补丁	×	√	√	√
	敏感目录、反弹Shell	×	√	√	√

功能		基础版（新）①	标准版	专业版（包周期）	专业版（按需）
	病毒防御AV	×	×	√	√
系统管理	多账号管理	×	20个	50个	20个

说明

标识说明：

- √：表示在当前版本中支持。
- ×：表示在当前版本中不支持。
- ①：基础版有新老两个版本，老版本（免费）已在2023年停止购买，新版本（计费）是2024年新发售的更新功能后的版本，**表 版本差异说明**中是新基础版支持的功能特性。

5 个人数据说明

使用个人数据的场景	日志数据	网络抓包
收集的个人数据项	IP地址	抓包文件
收集的来源和方式	防火墙通过防护的流量识别出的源IP地址和目的IP地址	在防火墙控制台上使用抓包功能
使用目的以及安全保护措施	• 向用户展示防火墙识别出的流量明细。 • 数据通过http上传到告警管理服务器。 • 明文存储，仅管理员可以访问。	用户在防火墙上进行流量抓包后存储到管理账号的OBS桶中，仅管理员可以访问。
存留期限与存留策略	满7天会自动删除	满7天会自动删除
销毁方式	系统直接删除，直接释放存储空间给其它数据使用	系统直接删除，直接释放存储空间给其它数据使用
导出方式	日志通过防火墙控制台导出。	使用提取码下载储存在OBS中的抓包文件。
导出指导	用户自行在“日志审计 > 日志查询”页面进行导出。	请参见**下载抓包结果**。

6 安全

6.1 责任共担

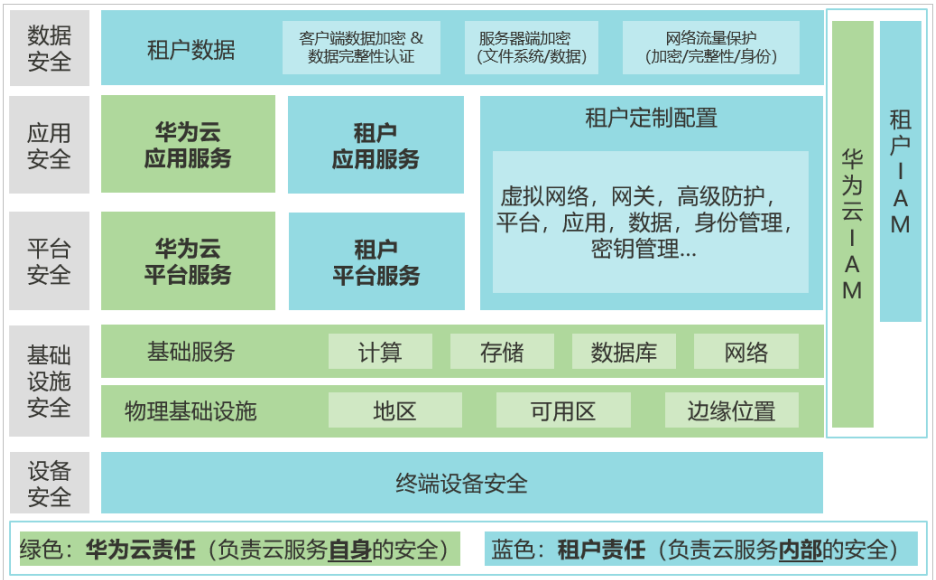
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图6-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 6-1 华为云安全责任共担模型



6.2 身份认证与访问控制

CFW对接了统一身份认证服务（Identity and Access Management，IAM）服务。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对华为云资源的访问范围。

关于对CFW资源的访问权限，详细请参考**CFW权限管理**。

6.3 数据保护技术

CFW通过多种数据保护手段和特性，保证通过CFW的数据安全可靠。

表 6-1 CFW 的数据保护手段和特性

数据保护手段	简要说明
静态数据保护	CFW通过敏感数据加密保证用户流量中敏感数据的安全性。
传输中的数据保护	微服务间管理数据传输进行加密，防止数据在传输过程中泄露或被篡改。用户的配置数据传输采用安全协议HTTPS，防止数据被窃取。
数据完整性校验	CFW进程启动时，配置数据从配置中心获取而非直接读取本地文件。
数据隔离机制	租户区与管理面隔离，租户的所有操作权限隔离，不同租户间的策略、日志等数据隔离。

数据保护手段	简要说明
数据销毁机制	考虑到残留数据导致的信息泄露问题，华为云根据客户等级设定了不同的保留期时长，保留期到期仍未续订或充值，存储在云服务中的数据将被删除，云服务资源将被释放。CFW对云服务自动感知并在保留期到期后释放资源。

同时，CFW服务充分尊重用户隐私，遵循法律法规。以入侵防护功能为例，CFW仅会对流量进行**威胁签名匹配检测**和**异常行为检测**，不会采集和存储任何用户隐私数据。更多隐私数据使用和保护问题，请参考**隐私政策声明**。

6.4 审计与日志

日志审计是保证云防火墙可靠性、可用性和性能的重要组成部分。用户可以汇总华为云服务的操作日志并进行分析、审计、资源监控和问题定位。

CFW已对接云审计服务（Cloud Trace Service, CTS）。华为云云审计服务提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

CTS的详细介绍和使用方法，请参见**CTS快速入门**。

6.5 服务韧性

华为云数据中心按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减少由硬件故障、自然灾害或其它灾难带来的服务中断，华为云为所有数据中心提供灾难恢复计划。

当发生故障时，CFW的五级可靠性架构支持不同层级的可靠性，因此具有更高的可用性、容错性和可扩展性。

华为云CFW已面向全球用户服务，并在多个分区部署，同时CFW的所有管理面、引擎等组件均采用主备或集群方式部署。分区部署详情参见**地区和终端节点**。

6.6 监控安全风险

CFW已对接云监控服务（Cloud Eye，CES）。该服务是华为云为用户提供一个针对各种云上资源的立体化监控平台，用户通过云监控服务可以全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

用户使用CES并创建监控指标后，用户可以通过CES管理控制台检索云防火墙产生的监控指标和告警信息。

- CES的详细介绍和使用方法，请参见**CES快速入门**。
- 如何使用CES对CFW进行监控，请参见**设置监控告警规则**。

6.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 6-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 6-3 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 6-4 销售许可证&软件著作权证书

7 权限管理

如果您需要对华为云上购买的云防火墙（CFW）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为账号中给员工创建IAM用户，并授权控制员工对云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些员工拥有云防火墙（CFW）的使用权限，但是不希望这些员工拥有删除CFW等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CFW，但是不允许删除CFW的权限策略，控制员工对华为云CFW资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CFW服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

CFW 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CFW部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问CFW时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其它角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CFW服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表7-1所示，包括了CFW下所有的系统角色。

表 7-1 CFW 系统角色

角色名称	描述	类别	依赖关系
CFW FullAccess	云防火墙服务的所有权限。	系统策略	无
CFW ReadOnlyAccess	云防火墙服务的只读权限。	系统策略	无

相关链接

- IAM产品介绍

CFW FullAccess 策略内容

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "cfw:*:*",
                "vpc:publicIps:list",
                "vpc:publicipTags:get",
                "vpc:vpcs:create",
                "vpc:vpcs:list",
                "vpc:vpcs:get",
                "vpc:subnets:get",
                "vpc:subnets:create",
                "vpc:routeTables:list",
                "vpc:routeTables:update",
                "vpc:quotas:list",
                "er:instances:list",
                "er:attachments:list",
                "er:attachments:create",
                "er:routeTables:list",
                "er:routes:list",
                "er:associations:list",
                "er:instances:get",
                "ecs:cloudServers:list",
                "ecs:availabilityZones:list",
                "smn:topic:list",
                "nat:natGateways:list",
                "lts:groups:list",
                "lts:topics:get",
                "dcaas:vgw:list",
                "eps:resources:list",
                "tms:predefineTags:list"
            ],
            "Effect": "Allow"
        }
    ]
}
```

CFW ReadOnlyAccess 策略内容

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
```

```
            "cfw:*:list",
            "cfw:*:get",
            "vpc:publicIps:list",
            "vpc:publicipTags:get",
            "vpc:vpcs:list",
            "vpc:vpcs:get",
            "vpc:subnets:get",
            "vpc:routeTables:list",
            "vpc:quotas:list",
            "er:instances:list",
            "er:attachments:list",
           "er:routeTables:list",
           "er:routeTables:list",
           "er:routes:list",
           "er:associations:list",
           "er:instances:get",
            "ecs:cloudServers:list",
            "ecs:availabilityZones:list",
            "smn:topic:list",
            "nat:natGateways:list",
            "lts:groups:list",
            "lts:topics:get",
            "dcaas:vgw:list",
            "eps:resources:list",
            "tms:predefineTags:list"
        ],
        "Effect": "Allow"
    }
  ]
}
```

特殊权限策略

CFW部分功能依赖于弹性云服务器（Elastic Cloud Server， ECS）、虚拟私有云（Virtual Private Cloud， VPC）等云服务，因这些云服务中部分功能不支持企业项目，将“CFW FullAccess” 和“CFW ReadOnlyAccess”两个系统策略授权到企业项目维度后会造成部分权限失效。

所以需要使用华为云账户自行创建两条系统策略，具体创建步骤请参见：**创建自定义策略**。

- CFW依赖的云服务中不支持企业项目的功能需要按照以下内容添加权限，其中云日志服务（Log Tank Service，简称LTS）在CFW页面操作时需授权LTS服务全部权限。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc:quotas:list",
            "vpc:publicipTags:get"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "ecs:availabilityZones:list"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "lts:groups:list",
            "lts:groups:get",
         ]
```

```
        }
    ]
}
```

- CFW依赖全局服务的权限：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "eps:resources:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "tms:predefineTags:list"
            ]
        }
    ]
}
```

8 约束与限制

本文介绍云防火墙CFW服务在使用过程中的约束和限制。

CFW 使用限制

- 仅支持对部署在华为云的业务提供防护，不支持跨云使用。
- 支持弹性公网IP EIP的流量防护，不支持全域公网带宽GEIP、API网关APIG绑定的EIP的流量防护。
- 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**功能总览**。
- VPC边界流量防护功能依赖企业路由器ER服务引流，使用该功能时，需确保账号下至少有一个企业路由器。
- 云防火墙不支持防护中文域名。
- 标准版旁路引擎已于2023年1月停止销售，相关功能在此之后停止演进，该版本不支持云监控服务CES、查看IPS库或修改IPS动作、日志存储至云日志服务LTS、病毒防御（专业版）等功能。如需使用以上功能建议切换为直路引擎。

防护策略配额限制

- 防护规则

  一个防火墙实例最多添加20000条防护规则。
- 黑白名单
  - 一个防火墙实例最多添加2000条黑名单。
  - 一个防火墙实例最多添加2000条白名单。
- 成员组
  - IP地址组
    - 每个防火墙实例下最多添加3800个IP地址组。
    - 每个IP地址组中最多添加640个IP地址成员。
    - 每个防火墙实例下最多添加30000个IP地址。
  - 服务组
    - 每个防火墙实例下最多添加900个服务成员。

    - 每个防火墙实例下最多添加512个服务组。
    - 每个服务组中最多添加64个服务成员。
  - 域名组
    - 基础版仅支持应用型域名组。
    - 域名组中所有域名被“防护规则”引用最多40,000次，泛域名被“防护规则”引用最多200次。
    - **应用域名组（七层协议解析）**
      - 每个防火墙实例下最多添加500个域名组。
      - 每个防火墙实例下最多添加2500个域名成员。
      - 每个应用域名组中最多添加1500个域名成员。
    - **网络域名组（四层协议解析）**
      - 每个防火墙实例下最多添加1000个域名成员。
      - 每个网络域名组中最多添加15个域名成员。
      - 每个域名组最多支持解析1500条IP地址。
      - 每个域名最多支持解析1000条IP地址。

基础防御 IPS 限制

- 修改基础防御规则动作
  - 最多可修改3000条规则为“观察”。
  - 最多可修改3000条规则为“拦截”。
  - 最多可修改128条规则为“禁用”。
- 自定义IPS特征
  - 仅专业版支持自定义IPS特征。
  - 最多支持添加500条特征。

日志数据限制

- 云防火墙支持查看7天以内的日志数据。将单类或者多类日志记录至LTS中，您可以查看1-365天的日志数据。
- 单个日志单次最多支持导出100,000条记录。
- 基础版不支持查询攻击事件日志。

9 与其它服务的关系

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为云防火墙服务提供了权限管理的功能。需要拥有Tenant Administrator权限的用户才能拥有CFW服务的操作权限（包括云资源授权，资产管理以及执行资产检测任务等）。如需开通该权限，请联系拥有Security Administrator权限的用户。

与弹性公网 IP 的关系

弹性公网IP（Elastic IP，简称EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。

云防火墙通过对弹性公网IP的防护实现互联网边界流量的防护。

与虚拟私有云的关系

虚拟私有云（Virtual Private Cloud，VPC）是您在云上的私有网络，为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。

云防火墙支持防护VPC边界的流量，例如VPC与VPC之间、云上VPC与云下IDC之间。

与 NAT 网关的关系

NAT网关（NAT Gateway）提供公网NAT网关和私网NAT网关。公网NAT网关为VPC内的云主机提供SNAT和DNAT功能，可轻松构建VPC的公网出入口。

云防火墙通过防护NAT网关所在的VPC，实现对NAT网关流量的防护。

与企业路由器的关系

企业路由器（Enterprise Router, ER）为云防火墙提供VPC间防护的引流能力。当用户购买专业版防火墙，对VPC间流量或专线流量进行防护时，需要通过ER服务进行引流。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）为云防火墙提供云服务资源的操作记录，记录内容包括从访问管理控制台发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

CTS记录了CFW相关的操作事件，方便用户日后的查询、审计和回溯。

与云监控服务的关系

云监控（Cloud Eye）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。用户可以通过云监控服务的相关指标及时了解云防火墙的防护状况，并根据这些指标调整防护规则。

与云日志服务的关系

云日志服务（Log Tank Service，LTS）用于收集来自主机和云服务的日志数据。云防火墙可以设置将攻击事件日志、访问控制日志、流量日志记录到LTS中，为您提供一个实时、高效、安全的日志处理功能。

与消息通知服务的关系

消息通知服务（Simple Message Notification，SMN）提供消息通知功能。用户在CFW开启通知设置后，资源受到攻击或防护流量超额时，会通过设置的接收通知方式收到告警信息。

与企业管理的关系

企业中有多个项目，多个项目的资源需要分开结算，且分属不同人员进行管理。同时项目可以单独启动或停止，对其它项目没有影响。**企业管理**可以针对企业中的每个项目，分别建立企业项目，管理各自的资源，并且针对不同的企业项目，设置不同的人员进行管理。

云防火墙支持企业管理，您可以将云防火墙上的资源按照企业项目进行管理，并设置每个企业项目的用户权限。

与 Web 应用防火墙的主要区别

云防火墙和Web应用防火墙是华为云推出的两款不同的产品，为您的互联网边界和VPC边界、Web服务提供防护。

CFW和WAF的主要区别说明如**表9-1**所示。

表 9-1 CFW 和 WAF 的主要区别说明

类别	云防火墙	Web应用防火墙
定义	云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	Web应用防火墙（Web Application Firewall，WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。 有关Web应用防火墙的详细介绍，请参见**什么是Web应用防火墙**。

类别	云防火墙	Web应用防火墙
防护对象	• 弹性公网IP和VPC边界。 • 支持对Web攻击的基础防护。 • 支持外部入侵和主动外联的流量防护。	• 针对域名或IP，华为云、非华为云或云下的Web业务。 • 支持对Web攻击的全面防护。
功能特性	• 资产管理与入侵防御：对已开放公网访问的服务资产进行安全盘点，进行实时入侵检测与防御。 • 访问控制：支持互联网边界访问流量的访问控制。 • 流量分析与日志审计：VPC间流量全局统一访问控制，全流量分析可视化，日志审计与溯源分析。	SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击防护。

10 等保合规能力说明

检查项分类	安全控制点	等保合规检查项	风险等级参考	云防火墙CFW提供的对应能力说明	相关功能介绍
安全通信网络	**网络架构**	应避免将重要网络区域部署在边界处，重要网络区域与其它网络区域之间应采取可靠的技术隔离手段。	高	通过云原生VPC能力，将重要网络区域使用VPC隔离，不同重要级别的VPC之间的业务互访，使用云防火墙CFW实现VPC间业务流量的访问控制，并对恶意访问进行识别和拦截。	**应用场景**
		应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。	中	通过云防火墙自动识别业务在互联网的威胁暴露面，提供云上互联网边界和VPC边界的防护，入侵防御引擎对恶意流量实时检测和拦截。	
安全区域边界	**边界防护**	应能够对内部用户非授权连到外部网络的行为进行限制或检查。	高	云防火墙实现南北向和东西向访问的网络流量分析、全网流量可视化、对主动外联行为的分析和阻断、开通或变更白名单策略。	**功能特性**
		应能够对非授权设备私自连到内部网络的行为进行限制或检查。	中		
		应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	中		

检查项分类	安全控制点	等保合规检查项	风险等级参考	云防火墙CFW提供的对应能力说明	相关功能介绍
	入侵防范	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。	高	云防火墙实现对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截。	
		应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。	高	云防火墙实现云上资产对外流量的主动外联、失陷感知等出方向流量分析和攻击防护及访问控制。	
		当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	中	云防火墙提供对业务流量中的攻击行为的检测和记录，并能根据策略设置提供攻击流量阻断功能，记录风险级别、事件名称、源IP、目的IP、方向、判断来源、发生时间和动作。	
	访问控制	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下受控接口拒绝除允许通信外的所有通信。	高	云防火墙实现统一管理互联网到业务的南北向访问策略和业务，达到协议、端口、应用级访问控制粒度。	**访问控制策略**
		应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。	中	云防火墙提供策略命中计数功能，客户可以根据命中情况，及时调整策略的设置，确保没有冗余的策略。云防火墙访问控制策略可配置优先级，您可以根据业务需求优化访问控制列表。	
		应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许或拒绝数据包进出。	高	云防火墙实现对进出访问控制策略进行严格设置。访问控制策略包括源类型、访问源、目的类型、目的、协议类型、目的端口、应用协议、动作、描述和优先级。	

检查项分类	安全控制点	等保合规检查项	风险等级参考	云防火墙CFW提供的对应能力说明	相关功能介绍
		应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。	中	云防火墙对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截。	
		应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	中	云防火墙实现跨VPC流量的应用协议、内容的访问控制。	
	安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	高	云防火墙提供日志审计功能，可以记录所有流量日志、事件日志和操作日志。	**日志审计功能**
		审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其它与审计相关的信息。	中	云防火墙提供日志记录事件功能，包括：时间、威胁类型、方向、源IP和目的IP、应用类型、严重性等级以及响应动作等信息。	
		应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	中	云防火墙提供日志分析功能，对已分析的日志，默认提供存储6个月内的日志数据，并提供实时日志分析能力。	
		应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	中	云防火墙提供日志分析功能，对已分析的日志，默认提供存储6个月内的日志数据，并提供实时日志分析能力。	

11 基本概念

五元组

五元组包括：源IP地址、目的IP地址、协议号、源端口、目的端口。

防护流量

入云流量：从Internet流入云防火墙方向的流量，例如，从公网下载资源到云内服务器。

出云流量：从云防火墙流出到Internet方向的流量，例如，云内服务器对外提供服务，外部用户下载云内的资源。

防护带宽：所有经过云防火墙防护的业务带宽。

互联网边界防护带宽：所有经过云防火墙防护的EIP的流量总和最大值，按照入云流量（入流量）或出云流量（出流量）的最大值取值。

VPC边界防护带宽：所有经过云防火墙防护的VPC的流量总和最大值。

互联网边界防火墙

互联网边界防火墙用于检测云资产与互联网之间的通信流量（即南北向流量），支持以弹性IP为防护对象的入侵检测防御（IPS）和网络防病毒（AV）功能，互联网边界防护的相关操作请参见**开启互联网边界流量防护**。

VPC 边界防火墙

VPC边界防火墙用于检测两个VPC之间的通信流量（即东西向流量），实现内部业务互访活动的可视化与安全防护，VPC边界防护的相关操作请参见**开启VPC边界流量防护**。

入侵防御系统

入侵防御系统（Intrusion Prevention System，IPS）位于防火墙和网络设备之间。如果检测到攻击，IPS会在攻击扩散到网络的其它地方之前阻止该恶意通信，IPS的相关介绍请参见**攻击防御功能概述**。

病毒防御

病毒防御（Anti-Virus，AV）通过病毒特征检测来识别和处理病毒文件，避免由病毒文件引起的数据破坏、权限更改和系统崩溃等情况发生，有效保护您的业务安全，病毒防御的相关操作请参见**拦截病毒文件**。

Internet 访问

Internet访问是指互联网IP访问云主机的行为，通过对Internet访问防护，可以帮助您及时防御外部入侵。

主动外联访问

主动外联访问是指云主机主动访问外部IP的行为，通过对主动外联访问防护，可以帮助您有效管理和控制主机外联行为。

企业路由器

企业路由器（Enterprise Router, ER）可以连接VPC或本地网络来构建中心辐射型组网，是云上大规格，高带宽，高性能的集中路由器。

云墙关联子网

云墙关联子网是VPC边界防火墙中的参数。用户配置网段后，云防火墙自动分配“云墙关联子网”，用于将防火墙方向的流量转发到企业路由器。

CVE 编号

CVE编号是识别漏洞的唯一标识符。

CVE (Common Vulnerabilities and Exposures，通用漏洞披露) 是安全漏洞列表，列表中的每个条目都会有一个唯一的CVE编号。

Inspection VPC

Inspection VPC是VPC边界防火墙中的引流VPC。用户配置网段后，云防火墙默认创建“Inspection VPC”，在“企业路由器”模式中用于企业路由器和防火墙之间引流。